# Table of Contents

**What is Amazon Connect?** .................................................................................................................. 1
  How to get started ................................................................................................................................. 1
  Pricing .................................................................................................................................................. 1
  Services to use with Amazon Connect ................................................................................................. 2
    Development ....................................................................................................................................... 2
    Storage ............................................................................................................................................... 3
    Database ............................................................................................................................................ 3
  Analytics ............................................................................................................................................... 3
  Machine Learning (ML) and Artificial Intelligence (AI) ....................................................................... 4
  Messaging ............................................................................................................................................ 4
  Security ................................................................................................................................................ 4
  Management ........................................................................................................................................ 5
**Supported Regions** ............................................................................................................................. 5
  Amazon Connect .................................................................................................................................. 6
  AppIntegrations .................................................................................................................................... 7
  Amazon Q in Connect ........................................................................................................................... 9
  Cases ................................................................................................................................................... 9
  Contact Lens ....................................................................................................................................... 10
  Customer Profiles ................................................................................................................................. 13
  Voice ID ............................................................................................................................................... 14
  Agent workspace .................................................................................................................................. 15
  Agent workspace third-party applications (Preview) .............................................................................. 16
  Chat messaging: SMS subtype .............................................................................................................. 16
  Communications widget ....................................................................................................................... 16
  In-app, web, and video calling capabilities ............................................................................................ 17
  Forecasting, capacity planning, and scheduling ..................................................................................... 17
  Live media streaming ............................................................................................................................ 17
  Outbound campaigns ............................................................................................................................. 18
  Tasks .................................................................................................................................................... 18
**Supported browsers** ............................................................................................................................ 19
  Mobile browsers .................................................................................................................................... 20
  Supported browsers and mobile OS for in-app, web, and video calling capabilities ......................... 20
  Issue with Firefox .................................................................................................................................. 21
**Supported screen readers** .................................................................................................................. 21
Supported languages .................................................................................................................. 21
Contact Control Panel ............................................................................................................. 22
Chat message content ............................................................................................................. 23
Amazon Connect admin website .............................................................................................. 23
Amazon Connect Cases .......................................................................................................... 23
Amazon Connect Contact Lens ............................................................................................... 24
Pattern match languages ....................................................................................................... 26
Amazon Connect forecasting, capacity planning, and scheduling ........................................ 26
Amazon Q in Connect ............................................................................................................. 27
Amazon Lex ............................................................................................................................ 27
Amazon Polly .......................................................................................................................... 27
Service quotas ......................................................................................................................... 27
Important things to know ....................................................................................................... 28
Amazon Connect quotas ......................................................................................................... 29
AppIntegrations quotas ........................................................................................................... 33
Amazon Q in Connect quotas ................................................................................................. 34
Cases quotas ........................................................................................................................... 35
Contact Lens quotas ............................................................................................................... 36
Customer Profiles quotas ...................................................................................................... 37
Outbound campaigns quotas .................................................................................................. 39
Voice ID quotas ....................................................................................................................... 39
How contacts are counted ...................................................................................................... 40
Feature specifications ............................................................................................................. 42
Countries you can call by default ........................................................................................... 52
API throttling quotas ............................................................................................................. 55

Get started .................................................................................................................................. 62
Next steps .................................................................................................................................. 62
Take a free online class ............................................................................................................. 63
Concepts ................................................................................................................................... 63
Telephony ................................................................................................................................. 64
Web and mobile messaging ...................................................................................................... 67
Tasks .......................................................................................................................................... 72
Routing profiles ....................................................................................................................... 79
Queues: standard and agent .................................................................................................... 81
Queues: priority and delay ....................................................................................................... 83
Queue-based routing ............................................................................................................... 86
Channels and concurrency ................................................................. 86
Flows ......................................................................................... 87
Best practices .................................................................................. 90
Flows ......................................................................................... 90
Lambda ......................................................................................... 91
Chat and Amazon Lex ....................................................................... 92
Contact Control Panel ..................................................................... 92
Tutorials .......................................................................................... 92
  Tutorial 1: Set up your Amazon Connect instance .................................. 93
  Tutorial 2: Test the sample voice and chat experience .............................. 104
  Tutorial 3: Create an IT help desk ...................................................... 110
Design for low latency ....................................................................... 139
Architectural guidance ....................................................................... 141
  Amazon Connect workload layers ...................................................... 141
  Scenario and deployment approaches .................................................. 147
  Operational Excellence .................................................................... 159
  Security ........................................................................................ 176
  Reliability ...................................................................................... 187
  Performance efficiency ..................................................................... 188
  Cost optimization ........................................................................... 197
Plan identity management .................................................................... 200
  Use an existing directory for identity management ................................. 201
  Configure SAML with IAM for Amazon Connect .................................... 202
  Troubleshoot SAML with Amazon Connect .......................................... 212
Additional resources ......................................................................... 216
  Amazon Connect API Reference ......................................................... 216
  Amazon Connect Participant Service API Reference .............................. 216
  Amazon AppIntegrations Service API Reference .................................... 216
  Contact Lens for Amazon Connect API Reference .................................... 216
  Amazon Connect Customer Profiles API ............................................. 217
  Amazon Connect Voice ID API Reference .......................................... 217
  Amazon Q in Connect API Reference .................................................. 217
  Amazon Connect Streams ................................................................... 217
  Amazon Connect Chat UI Examples .................................................... 217
  Administrative support ....................................................................... 217

**Set up your contact center** ................................................................ 219
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up outbound caller ID</td>
<td>420</td>
</tr>
<tr>
<td>Set up US emergency calling</td>
<td>426</td>
</tr>
<tr>
<td>Enable outbound calls</td>
<td>434</td>
</tr>
<tr>
<td>Outbound calling restrictions</td>
<td>436</td>
</tr>
<tr>
<td>Optimize your reputation for outbound calling</td>
<td>438</td>
</tr>
<tr>
<td>Enable Amazon Connect outbound campaigns</td>
<td>441</td>
</tr>
<tr>
<td>Create an outbound campaign</td>
<td>444</td>
</tr>
<tr>
<td>Disable outbound campaigns</td>
<td>448</td>
</tr>
<tr>
<td>Assign permissions</td>
<td>448</td>
</tr>
<tr>
<td>Add users</td>
<td>449</td>
</tr>
<tr>
<td>Add users</td>
<td>450</td>
</tr>
<tr>
<td>Edit users in bulk</td>
<td>455</td>
</tr>
<tr>
<td>View historical changes</td>
<td>460</td>
</tr>
<tr>
<td>Download users</td>
<td>462</td>
</tr>
<tr>
<td>Delete users</td>
<td>462</td>
</tr>
<tr>
<td>Reset passwords</td>
<td>466</td>
</tr>
<tr>
<td>Security profiles</td>
<td>467</td>
</tr>
<tr>
<td>Set up routing</td>
<td>508</td>
</tr>
<tr>
<td>How routing works</td>
<td>508</td>
</tr>
<tr>
<td>Create a queue</td>
<td>510</td>
</tr>
<tr>
<td>Disable a queue</td>
<td>512</td>
</tr>
<tr>
<td>Delete a queue</td>
<td>513</td>
</tr>
<tr>
<td>Set queue capacity</td>
<td>513</td>
</tr>
<tr>
<td>Set the hours of operation</td>
<td>517</td>
</tr>
<tr>
<td>Create a routing profile</td>
<td>520</td>
</tr>
<tr>
<td>Delete a routing profile</td>
<td>527</td>
</tr>
<tr>
<td>Set up queue-based routing</td>
<td>527</td>
</tr>
<tr>
<td>Set up agents</td>
<td>527</td>
</tr>
<tr>
<td>Set up agent hierarchies</td>
<td>528</td>
</tr>
<tr>
<td>Customize agent status</td>
<td>530</td>
</tr>
<tr>
<td>Configure agent settings</td>
<td>531</td>
</tr>
<tr>
<td>Enable auto-accept call</td>
<td>533</td>
</tr>
<tr>
<td>CCPv1: Set up automatic agent logout</td>
<td>535</td>
</tr>
<tr>
<td>Set up agents to assign tasks to themselves</td>
<td>537</td>
</tr>
<tr>
<td>Set up tasks</td>
<td>538</td>
</tr>
<tr>
<td>Create task templates</td>
<td>539</td>
</tr>
</tbody>
</table>
Assign permissions for creating task templates ........................................ 544
Block agents from creating tasks .......................................................... 544
Set up applications for task creation ....................................................... 544
Create rules .............................................................................................. 564
Set up in-app, web, and video calling capabilities .................................. 567
Communication widget ............................................................................ 568
How to set up in-app, web, and video calling .......................................... 569
Option 1: Configure an out-of-the-box communication widget ............... 569
Option 2: Integrate in-app, web, and video calling natively into your mobile application .. 575
Passing attributes ...................................................................................... 578
Integrate video calling into your custom agent desktop .......................... 583
Set up your customer's chat experience ................................................... 585
More resources .......................................................................................... 586
Add a chat user interface to your website .................................................. 586
Create quick responses ............................................................................. 615
Enable text formatting ................................................................................ 627
Enable message Delivered and Read receipts ......................................... 630
Set up chat timeouts .................................................................................. 631
Enable persistent chat ............................................................................... 635
Enable Apple Messages for Business ...................................................... 641
Enable real-time message streaming ....................................................... 661
Customize chat flow experiences ............................................................ 669
Set up SMS messaging ............................................................................. 671
  Step 1: Request a number in Amazon Pinpoint SMS ............................. 672
  Step 2: Enable two-way SMS on the phone number ............................. 674
  Step 3: Update flows to branch on SMS contacts ................................. 676
  Step 4: Test sending and receiving SMS messages ............................. 679
Next steps ................................................................................................. 680
Upgrade to the latest CCP ........................................................................ 680
  Upgrade on your own schedule, before your automatic upgrade date ........ 680
  Upgrade later, automatically ............................................................... 680
  My CCP URL ends with /ccp# ............................................................. 681
    I use the Amazon Connect Streams API ......................................... 694
Provide access to the CCP ....................................................................... 696
Steps to ensure agents can access the CCP ........................................... 696
Agent application: Everything in one place .......................................... 697
Grant microphone access in Chrome, Firefox, or Edge ........................................... 697
How to get help for CCP issues .............................................................................. 698
Headset and workstation requirements ................................................................. 698
Can't hear caller or caller can't hear agent? ......................................................... 700
Agents can't hear indicator for incoming chat? ..................................................... 701
Embed a custom CCP ............................................................................................ 702
Use Amazon Connect Streams API for third-party cookies ............................... 702
Embed CCP into Salesforce .................................................................................. 710
Embed CCP into Zendesk .................................................................................... 711

**Set up Amazon Connect Global Resiliency** ....................................................... 712
Get started .............................................................................................................. 713
How to set up Amazon Connect Global Resiliency .............................................. 713
Create a replica of your existing Amazon Connect instance ............................... 714
Create traffic distribution groups ......................................................................... 719
Claim phone numbers to traffic distribution groups ............................................. 720
Assign claimed phone numbers to traffic distribution groups ......................... 723
Update telephony traffic distribution across AWS Regions ................................. 725
Set up your agent's experience ........................................................................... 726
Manage traffic distribution groups ...................................................................... 738
List traffic distribution groups .............................................................................. 739
Delete traffic distribution groups ......................................................................... 739
Manage phone numbers across Regions .............................................................. 739
Claim phone numbers to instances across multiple AWS Regions .................. 740
Move a claimed phone number to multiple instances across AWS Regions .... 740
Release numbers from traffic distribution groups ................................................. 741

**Set up your network** .......................................................................................... 742
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist .......................................................... 743
  NLB endpoints .................................................................................................... 750
Option 2 (not recommended): Allow IP address ranges ....................................... 752
About Amazon Connect IP address ranges .......................................................... 753
Stateless firewalls ................................................................................................. 754
Allow DNS resolution for softphones .................................................................. 754
Port and protocol considerations ......................................................................... 755
Region selection considerations .......................................................................... 756
Agents using Amazon Connect remotely ............................................................ 757
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rerouting audio</td>
<td>757</td>
</tr>
<tr>
<td>Using AWS Direct Connect</td>
<td>757</td>
</tr>
<tr>
<td>Agent workstation networking requirements for web calling voice/video</td>
<td>757</td>
</tr>
<tr>
<td>Detailed Network Paths</td>
<td>759</td>
</tr>
<tr>
<td>Voice calls</td>
<td>759</td>
</tr>
<tr>
<td>Authentication</td>
<td>760</td>
</tr>
<tr>
<td>Using Amazon Connect in a VDI environment</td>
<td>761</td>
</tr>
<tr>
<td>CCP connectivity</td>
<td>762</td>
</tr>
<tr>
<td>Use an allowlist for integrated applications</td>
<td>764</td>
</tr>
<tr>
<td>Update your domain</td>
<td>764</td>
</tr>
<tr>
<td>Firewall allow list</td>
<td>765</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>765</td>
</tr>
<tr>
<td>Custom code and integrations</td>
<td>766</td>
</tr>
<tr>
<td>API endpoint access</td>
<td>767</td>
</tr>
<tr>
<td>Personal settings</td>
<td>768</td>
</tr>
<tr>
<td><strong>Create flows</strong></td>
<td>769</td>
</tr>
<tr>
<td>Required permissions</td>
<td>769</td>
</tr>
<tr>
<td>Default flows</td>
<td>770</td>
</tr>
<tr>
<td>Change a default contact flow</td>
<td>771</td>
</tr>
<tr>
<td>Default agent hold</td>
<td>775</td>
</tr>
<tr>
<td>Default agent transfer</td>
<td>777</td>
</tr>
<tr>
<td>Default customer queue</td>
<td>777</td>
</tr>
<tr>
<td>Default customer whisper</td>
<td>780</td>
</tr>
<tr>
<td>Default agent whisper</td>
<td>780</td>
</tr>
<tr>
<td>Set the default whisper flow for chat</td>
<td>781</td>
</tr>
<tr>
<td>Default customer hold</td>
<td>782</td>
</tr>
<tr>
<td>Default outbound</td>
<td>783</td>
</tr>
<tr>
<td>Default queue transfer</td>
<td>783</td>
</tr>
<tr>
<td>Default prompts from Amazon Lex</td>
<td>784</td>
</tr>
<tr>
<td>Sample flows</td>
<td>784</td>
</tr>
<tr>
<td>Sample inbound flow</td>
<td>785</td>
</tr>
<tr>
<td>Sample AB test</td>
<td>786</td>
</tr>
<tr>
<td>Sample customer queue priority</td>
<td>787</td>
</tr>
<tr>
<td>Sample disconnect flow</td>
<td>788</td>
</tr>
<tr>
<td>Sample queue configurations</td>
<td>789</td>
</tr>
<tr>
<td>Sample queue customer</td>
<td>792</td>
</tr>
</tbody>
</table>
Set disconnect flow ................................................................. 926
Set event flow ........................................................................ 928
Set hold flow .......................................................................... 931
Set logging behavior ................................................................ 933
Set recording and analytics behavior ....................................... 934
Set Voice ID ........................................................................... 938
Set voice ................................................................................. 944
Set whisper flow ..................................................................... 947
Set working queue .................................................................. 950
Show view ............................................................................... 952
Start media streaming ............................................................. 958
Stop media streaming ............................................................. 960
Store customer input .............................................................. 962
Transfer to agent (beta) .......................................................... 967
Transfer to flow ........................................................................ 969
Transfer to phone number ..................................................... 971
Transfer to queue ..................................................................... 975
Wait ......................................................................................... 980
Create a flow ........................................................................... 983
Before you begin: develop a naming convention .................... 984
Choose a flow type ................................................................... 984
Create an inbound flow .......................................................... 987
Use the mini-map to navigate a flow ....................................... 989
Customize the name of a block .............................................. 990
Undo and redo history ............................................................ 992
Add notes to a block ................................................................ 993
Copy and paste flows ............................................................ 995
Archive, delete, and restore flows .......................................... 997
Generate logs ........................................................................... 1000
Roll back a flow ...................................................................... 1001
Contact initiation methods and flow types ............................. 1002
Associate a phone number with a flow ................................. 1007
Flow modules ........................................................................... 1008
Where you can use modules .................................................. 1009
Limitations .............................................................................. 1009
Security profile permissions for modules .............................. 1010
Create a module ........................................................................................................... 1010
Add a module to a flow ............................................................................................. 1010
Example module ....................................................................................................... 1010
Create prompts .......................................................................................................... 1011
How to create prompts ............................................................................................... 1012
Supported file types .................................................................................................. 1013
Maximum length for prompts ..................................................................................... 1013
Bulk upload of prompts not supported in UI, API, or CLI ........................................ 1013
Add text-to-speech to prompts ................................................................................... 1013
Create dynamically text strings in Play prompt blocks .............................................. 1016
Dynamically select which prompts to play ............................................................... 1017
Set up prompts to play from an S3 bucket ................................................................. 1019
Choose the voice for audio prompts ........................................................................ 1022
Use SSML tags to personalize text-to-speech ........................................................... 1022
SSML tags aren't interpreted in chats ....................................................................... 1023
SSML tags supported by Amazon Connect ............................................................... 1024
Set up contact transfers ............................................................................................ 1025
Overview of steps ...................................................................................................... 1026
Create quick connects ............................................................................................... 1026
Delete quick connects ............................................................................................... 1031
How quick connects work .......................................................................................... 1032
Set up agent-to-agent transfers ................................................................................. 1035
Resume a flow after transfer ..................................................................................... 1038
Manage contacts in a queue ....................................................................................... 1040
Transfer contacts to agent queue ................................................................................ 1042
Set up recording behavior ........................................................................................ 1044
When is a conversation recorded? ............................................................................ 1045
Where are recordings stored? .................................................................................... 1045
When are recordings available? ................................................................................ 1046
Headset requirements ............................................................................................... 1047
How to set up recording behavior ........................................................................... 1047
How to set up users ................................................................................................... 1048
How to set up S3 Object Lock for immutable call recordings .................................... 1048
Set up queued callback ............................................................................................ 1051
Steps to set up queued callback ................................................................................. 1051
The routing process ................................................................................................... 1052
How queued callbacks affect queue limits .......................................................... 1053
Create a flow for queued callbacks ................................................................. 1053
Learn more about queued callbacks ............................................................... 1058
Import/export flows ......................................................................................... 1058
    Export limitations .......................................................................................... 1059
    Flows are exported to JSON files .................................................................. 1059
    How to import/export flows ......................................................................... 1059
    Resolve resources in imported contact flows ................................................. 1060
Add an Amazon Lex bot ....................................................................................... 1061
    Create an Amazon Lex bot ........................................................................... 1062
    Configure the Amazon Lex bot .................................................................... 1063
    Build and test the Amazon Lex bot .............................................................. 1068
    Create a bot version (Optional) ................................................................. 1071
    Create an alias for the bot .......................................................................... 1072
    Add the Amazon Lex bot to your Amazon Connect instance .................... 1073
    Create a flow and add your Amazon Lex bot .............................................. 1075
    Assign the flow to a phone number ............................................................ 1079
    Try it! .......................................................................................................... 1080
    Add interactive messages to chat .............................................................. 1080
Invoke Lambda functions .................................................................................. 1106
    Create a Lambda function ......................................................................... 1107
    Add a function to your instance .................................................................. 1107
    Invoke a Lambda from a flow ..................................................................... 1108
    Configure your function to parse the event .............................................. 1113
    Verify the function response .................................................................... 1114
    Consume the response ............................................................................. 1117
    Tutorial: Create a Lambda function and invoke in a flow ......................... 1120
Live media streaming of customer audio ......................................................... 1132
    Plan for live media streaming .................................................................... 1132
    Enable live media streaming ..................................................................... 1134
    Access Kinesis Video Streams Data .......................................................... 1134
    Test live media streaming ......................................................................... 1141
    Contact attributes for live media streaming ............................................. 1143
Encrypt customer input .................................................................................. 1144
    How to decrypt data encrypted by Amazon Connect .................................. 1145
Track events in flows ....................................................................................... 1147
Storage for flow logs ................................................................. 1147
Enable flow logs ................................................................. 1148
Search flow logs ................................................................. 1150
Data in flow logs .................................................................. 1152
Track customers between flows ............................................. 1153
Create alerts for flow log events ............................................. 1153
Use contact attributes .......................................................... 1154
  What is a contact attribute? ................................................. 1154
  List of attributes and their JSONPath reference ................. 1158
How to reference contact attributes ..................................... 1200
Display contact information to the agent ............................ 1201
Route based on number of contacts in a queue ...................... 1202
Route based on contact's channel ........................................ 1206
Use Amazon Lex and attributes ........................................... 1207
Lambda functions and attributes ........................................... 1211
Migrate flows ....................................................................... 1213

Real-time and historical metrics dashboards and reports .......... 1215

Dashboards .......................................................................... 1216
  Contact Lens conversational analytics dashboard .............. 1216
Queue performance dashboard .............................................. 1225
Required permissions ........................................................... 1230
Real-time metrics reports ....................................................... 1231
  Real-time metrics definitions ............................................. 1232
Required permissions ........................................................... 1245
Real-time metrics tag-based access control ......................... 1246
How often real-time metrics refresh ...................................... 1250
Use one-click drill-downs .................................................... 1250
Visualize: Queue dashboard .................................................. 1253
View contacts in queue ........................................................ 1255
Create a real-time metrics report ........................................... 1258
No metrics or too few rows? .................................................. 1259
List queues by routing profile ................................................. 1260
List agents by routing profile ................................................ 1261
Sort agents by activity .......................................................... 1262
Change an agent's activity status .......................................... 1263
Download a real-time metrics report .................................... 1265
Amazon Connect

Administrator Guide

Historical metrics reports .................................................................................. 1266
    Historical metrics definitions ........................................................................ 1267
    Required permissions .................................................................................... 1302
    Tag-based access control ............................................................................ 1303
    Create a historical metrics report ................................................................. 1303
    Report limits .................................................................................................. 1306
    Schedule a historical metrics report .............................................................. 1307
    Update a historical metrics report ................................................................ 1309
    Download a historical metrics report ........................................................... 1310
    Show agent queues in a Queues table .......................................................... 1312
    How many contacts in queue on a specific date ........................................... 1314
    Agent activity audit report ........................................................................... 1314

Login/Logout reports ............................................................................................ 1318
    Report limit .................................................................................................... 1319
    Required permissions .................................................................................... 1319
    Generate a Login/Logout report .................................................................... 1320
    Edit a Saved Login/Logout Report ................................................................. 1321
    Download a Login/Logout report as a CSV File ........................................... 1322
    Share a Login/Logout report ........................................................................ 1322
    Schedule a Login/Logout report .................................................................... 1323
    Delete a Saved Login/Logout report .............................................................. 1324
    Tag-based access control ............................................................................. 1324

Agent event streams ............................................................................................ 1325
    Enable agent event streams ......................................................................... 1325
    Sample agent event stream ......................................................................... 1326
    Determine how long an agent spends doing ACW ...................................... 1330
    Agent event streams data model .................................................................. 1337

Contact events .................................................................................................... 1346
    Subscribe to Amazon Connect contact events ............................................. 1346
    Contact events data model .......................................................................... 1349
    Contact timestamps ...................................................................................... 1355
    Sample to stop streaming an event type ....................................................... 1356
    Sample contact event for when a voice call is connected to an agent ........... 1357
    Sample contact event for when a voice call is disconnected ......................... 1358
    Sample contact data updated event ............................................................... 1359
    Contact records data model .......................................................................... 1361
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important things to know</td>
<td>1361</td>
</tr>
<tr>
<td>Agent</td>
<td>1362</td>
</tr>
<tr>
<td>AgentHierarchyGroup</td>
<td>1364</td>
</tr>
<tr>
<td>AgentHierarchyGroups</td>
<td>1365</td>
</tr>
<tr>
<td>ContactDetails</td>
<td>1366</td>
</tr>
<tr>
<td>ContactTraceRecord</td>
<td>1366</td>
</tr>
<tr>
<td>DeviceInfo</td>
<td>1374</td>
</tr>
<tr>
<td>DisconnectDetails</td>
<td>1375</td>
</tr>
<tr>
<td>Endpoint</td>
<td>1375</td>
</tr>
<tr>
<td>ExternalThirdParty</td>
<td>1376</td>
</tr>
<tr>
<td>MediaStream</td>
<td>1376</td>
</tr>
<tr>
<td>QualityMetrics</td>
<td>1376</td>
</tr>
<tr>
<td>QueueInfo</td>
<td>1377</td>
</tr>
<tr>
<td>RecordingInfo</td>
<td>1378</td>
</tr>
<tr>
<td>RecordingsInfo</td>
<td>1378</td>
</tr>
<tr>
<td>References</td>
<td>1380</td>
</tr>
<tr>
<td>RoutingProfile</td>
<td>1381</td>
</tr>
<tr>
<td>stateTransitions</td>
<td>1381</td>
</tr>
<tr>
<td>VoicedResult</td>
<td>1382</td>
</tr>
<tr>
<td>Authentication</td>
<td>1382</td>
</tr>
<tr>
<td>FraudDetection</td>
<td>1383</td>
</tr>
<tr>
<td>How to identify abandoned contacts</td>
<td>1385</td>
</tr>
<tr>
<td>View a contact record in the UI</td>
<td>1385</td>
</tr>
<tr>
<td>About agent status</td>
<td>1386</td>
</tr>
<tr>
<td>About custom agent statuses</td>
<td>1387</td>
</tr>
<tr>
<td>About ACW (After contact work)</td>
<td>1387</td>
</tr>
<tr>
<td>How do you know when an agent can handle another contact?</td>
<td>1388</td>
</tr>
<tr>
<td>What appears in the real-time metrics report?</td>
<td>1388</td>
</tr>
<tr>
<td>What appears in the agent event stream?</td>
<td>1388</td>
</tr>
<tr>
<td>&quot;We couldn't find this agent. Use the agent's user name to identify them.&quot;</td>
<td>1388</td>
</tr>
<tr>
<td>About contact states</td>
<td>1389</td>
</tr>
<tr>
<td>Contact states in the agent event stream</td>
<td>1389</td>
</tr>
<tr>
<td>Events in the contact record</td>
<td>1391</td>
</tr>
<tr>
<td>About queued callbacks</td>
<td>1392</td>
</tr>
<tr>
<td>How properties in the Transfer to Queue block affect this flow</td>
<td>975</td>
</tr>
<tr>
<td>Scheduled vs In queue</td>
<td>1394</td>
</tr>
</tbody>
</table>
Failed callback attempts ................................................................. 1396
Example: Metrics for a queued callback ........................................... 1397
Save custom reports ........................................................................ 1400
Personal saved reports count towards quota ..................................... 1400
Create a naming convention ............................................................. 1400
How to save reports ......................................................................... 1400
How to delete saved reports ............................................................. 1401
Share custom reports ........................................................................ 1402
View a shared report ......................................................................... 1404
  Tips for viewing a shared report ....................................................... 1405
Publish reports ................................................................................ 1405
  View published reports ................................................................... 1406
Manage saved reports (admin) ............................................................ 1407
  View and delete reports .................................................................. 1407
Monitor CloudWatch metrics ............................................................... 1408
  Amazon Connect metrics sent to CloudWatch .................................. 1409
  Amazon Connect CloudWatch metrics dimensions ............................. 1421
  Amazon Connect Voice ID metrics sent to CloudWatch ..................... 1423
  Amazon Connect Voice ID metrics dimensions .................................. 1425
  Amazon AppIntegrations metrics sent to CloudWatch ....................... 1426
  Amazon AppIntegrations metric dimensions ...................................... 1428
  Amazon Connect Customer Profiles metrics ...................................... 1428
  Amazon Connect Customer Profiles metric dimensions ..................... 1429
  Use CloudWatch metrics to calculate concurrent call quota ............... 1429
  Use CloudWatch metrics to calculate concurrent active chats quota ..... 1430
  Use CloudWatch metrics to calculate concurrent task quota .............. 1430
Logging service API calls .................................................................. 1431
  Amazon Connect information in CloudTrail .................................... 1431
  Example: Amazon Connect log file entries ...................................... 1432
  Example: Amazon Connect Voice ID log file entries .......................... 1433
EventBridge events emitted by Amazon Connect .................................. 1435
Analytics data lake (Preview) .............................................................. 1435
  Access Analytics data lake ............................................................... 1436
  Available tables ............................................................................ 1437
Agent Workspace ............................................................................... 1439
Step-by-step Guides .......................................................................... 1441
Overview ............................................................................................................. 1442
Complex JSON Object support ............................................................................. 1442
Enable step-by-step guides ................................................................................. 1442
View resource ....................................................................................................... 1444
Custom views ....................................................................................................... 1444
AWS managed views ............................................................................................ 1448
HTML and JSX support ....................................................................................... 1467
No-code UI builder ............................................................................................... 1468
UI component library ........................................................................................... 1468
Customize panel .................................................................................................... 1471
Setting actions that appear in flows .................................................................... 1482
Saving and publishing view versions ................................................................... 1484
Templates to get started quickly .......................................................................... 1484
Sample data .......................................................................................................... 1486
How to invoke a guide at the start of a contact ................................................. 1486
Display contact attributes in the agent workspace ............................................. 1488
Disposition codes ................................................................................................ 1488
PII Redaction ........................................................................................................ 1489
Third-party applications (Preview) .................................................................... 1490
Onboard third-party applications ........................................................................ 1490
Assign permissions ............................................................................................... 1495
Access third-party applications in the agent workspace .................................. 1496
Third-party application SSO Federation setup .................................................... 1498

Amazon Connect ................................................................................................... 1500
Enable Amazon Connect ....................................................................................... 1501
Before you begin ................................................................................................. 1502
Step 1: Add integration ....................................................................................... 1503
Step 2: Select object and fields .......................................................................... 1509
Step 3: Review and integrate .............................................................................. 1510
Step 4: Configure your flow for Amazon Connect ............................................. 1511
When was your knowledge base last updated? ................................................ 1512
Assign permissions ............................................................................................. 1512
Access Amazon Q in Connect in the agent application .................................... 1512

Cases ..................................................................................................................... 1514
Getting started with Cases .................................................................................. 1514
Enable Cases ........................................................................................................ 1515
Amazon Connect

Enable Contact Lens .................................................................................................................. 1552
Sample Contact details page for real-time chat analytics ......................................................... 1552
Sample Contact details page for post-chat analytics ................................................................. 1552
Enable Contact Lens .................................................................................................................. 1555
Assign permissions .................................................................................................................... 1568

Contact Lens ............................................................................................................................. 1549
Analyze conversations using conversational analytics ........................................................... 1550
Sample Contact details page for a call ..................................................................................... 1550
Sample Contact details page for real-time chat analytics ....................................................... 1552
Sample Contact details page for post-chat analytics ............................................................... 1552
Assign permissions .................................................................................................................... 1568

Requirements ............................................................................................................................. 1515
How to enable Cases .................................................................................................................. 1516
Next steps .................................................................................................................................... 1516
Assign permissions .................................................................................................................... 1517
Required Cases permissions ........................................................................................................ 1517
Required Customer Profiles permissions .................................................................................. 1517
Required queue, quick connect, and user view permissions ..................................................... 1518
Description of Cases permissions ............................................................................................... 1518
Required permissions for custom IAM policies .......................................................................... 1520
View Cases domain details ......................................................................................................... 1520
Onboard to Cases ....................................................................................................................... 1522
Create case fields ...................................................................................................................... 1525
How to create case fields ........................................................................................................... 1525
System case fields ..................................................................................................................... 1526
Custom case fields ..................................................................................................................... 1529
Create case templates ................................................................................................................ 1531
How case templates look in the agent application ....................................................................... 1532
How to create a template ........................................................................................................... 1533
Case layouts ................................................................................................................................ 1534
Set up case assignment .............................................................................................................. 1535
Set up agents and flows ............................................................................................................. 1536
How agents assign case ownership ............................................................................................ 1536
How to configure the Cases block to assign case ownership in a flow ..................................... 1539
Access Cases in the agent application ....................................................................................... 1540
Option 1: Use Cases with the CCP out-of-the-box ...................................................................... 1540
Option 2: Embed Cases into a custom agent application ............................................................ 1540
Case event streams .................................................................................................................... 1541
Set up case event streams .......................................................................................................... 1541
Case event payload and schema ................................................................................................. 1545

Administrator Guide
FAQ for screen recording capabilities ................................................................. 1760
Search for contacts .............................................................................................. 1762
  Important things to know .................................................................................. 1762
Key search features ............................................................................................. 1763
Required permissions .......................................................................................... 1765
How to search for a contact ................................................................................ 1768
Additional fields: Add columns to your search results ..................................... 1768
Download search results ................................................................................... 1769
Search for in-progress contacts ......................................................................... 1769
Search by custom contact attributes ................................................................... 1772
Monitor live & recorded conversations ............................................................... 1775
  Set up live monitoring for voice and/or chat ..................................................... 1776
Assign permissions .............................................................................................. 1777
Monitor live conversations .................................................................................. 1778
Barge live conversations ..................................................................................... 1780
Review recorded conversations ......................................................................... 1784
Troubleshoot monitoring conversations ............................................................ 1793
Manage contacts from the Contact details page ................................................ 1800
  Transfer contacts .............................................................................................. 1800
Reschedule contacts .......................................................................................... 1803
End contacts ....................................................................................................... 1805

**Customer Profiles** ....................................................................................... 1807

  What is a customer profile? .............................................................................. 1808
    Data storage ....................................................................................................... 1808
Enable Customer Profiles for your instance ..................................................... 1809
  Before you begin ............................................................................................... 1809
  Enable Customer Profiles, and specify a dead-letter queue and KMS key ...... 1811
  Next steps ............................................................................................................ 1821
Access Customer Profiles in the agent workspace ............................................ 1821
  Option 1: Use Customer Profiles with the CCP out-of-the-box ....................... 1821
  Option 2: Embed Customer Profiles into a custom agent workspace ............ 1823
Use contact attributes to autopopulate customer profiles ................................ 1824
  Automatically associate a customer profile with a contact ......................... 1825
Assign permissions ............................................................................................. 1826
  How update permissions for agents ......................................................... 1826
  How update permissions for Flows ................................................................. 1827
How update permissions for Calculated Attributes .......................................................... 1827
Issue with permissions: How to assign new permissions ................................................... 1828
Use Identity Resolution to consolidate similar profiles ...................................................... 1831
Enable Identity Resolution ................................................................................................ 1832
Machine learning for Identity Resolution ........................................................................ 1835
Rule-based matching for Identity Resolution .................................................................... 1845
Identity Resolution metrics .............................................................................................. 1858
Disable Identity Resolution .............................................................................................. 1860
Integrate external applications .......................................................................................... 1860
Set up integrations ............................................................................................................. 1861
Set up integration for featured applications in Amazon Connect ....................................... 1861
Set up integration for external applications using Amazon AppFlow ................................ 1887
Delete/stop Customer Profiles integrations ..................................................................... 1901
Object type mapping ........................................................................................................ 1902
Concepts and terminology for customer object type mappings ........................................ 1902
Create an object type mapping ........................................................................................ 1903
Object type mapping definition details ............................................................................ 1912
Additional properties of object types .............................................................................. 1972
Inferred profiles ................................................................................................................ 1972
Contact record templates .................................................................................................. 1973
Automatically associate the Contact Record with one profile found using the _phone
key .................................................................................................................................. 1978
Examples of object type mappings ................................................................................... 1979
Implicit profile object types ............................................................................................... 1982
Generative AI powered data mapping .............................................................................. 1983
Create and ingest customer data using Amazon S3 ......................................................... 1988
Set up real-time export ...................................................................................................... 1989
Enable real-time export ...................................................................................................... 1989
Enable real-time export ...................................................................................................... 1990
Real-time export Kinesis payload ...................................................................................... 1991
Real-time export troubleshooting ....................................................................................... 1993
Delete Customer Profiles domain .................................................................................... 1994
Customer Profiles Calculated Attributes ........................................................................ 1996
Calculated Attributes APIs ............................................................................................... 1997
Creating a custom calculated attribute definition ............................................................. 2012
Validating calculated attribute values using the API ......................................................... 2015
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Calculated Attributes</td>
<td>2017</td>
</tr>
<tr>
<td>Error state and troubleshooting</td>
<td>2022</td>
</tr>
<tr>
<td>Amazon Connect admin website</td>
<td>2022</td>
</tr>
<tr>
<td>How to create Calculated Attributes</td>
<td>2022</td>
</tr>
<tr>
<td>How to view Calculated Attributes</td>
<td>2026</td>
</tr>
<tr>
<td>How to edit Calculated Attributes</td>
<td>2027</td>
</tr>
<tr>
<td>How to delete Calculated Attributes</td>
<td>2029</td>
</tr>
<tr>
<td>Use the Customer Profiles API</td>
<td>2029</td>
</tr>
<tr>
<td>Example: Integrate with S3</td>
<td>2030</td>
</tr>
<tr>
<td><strong>Forecasting, capacity planning, and scheduling</strong></td>
<td>2033</td>
</tr>
<tr>
<td>Get started</td>
<td>2034</td>
</tr>
<tr>
<td>Enable forecasting, capacity planning, and scheduling</td>
<td>2034</td>
</tr>
<tr>
<td>Assign permissions</td>
<td>2037</td>
</tr>
<tr>
<td>Troubleshooting forecasting, capacity planning, and scheduling</td>
<td>2038</td>
</tr>
<tr>
<td>Forecasting</td>
<td>2047</td>
</tr>
<tr>
<td>Getting started with forecasting</td>
<td>2048</td>
</tr>
<tr>
<td>Set the forecast and scheduling interval</td>
<td>2049</td>
</tr>
<tr>
<td>Create forecast groups</td>
<td>2050</td>
</tr>
<tr>
<td>Import historical data</td>
<td>2052</td>
</tr>
<tr>
<td>Data requirements for forecasting</td>
<td>2057</td>
</tr>
<tr>
<td>Create forecasts</td>
<td>2058</td>
</tr>
<tr>
<td>Inspect a forecast</td>
<td>2059</td>
</tr>
<tr>
<td>Download a forecast</td>
<td>2060</td>
</tr>
<tr>
<td>Override a forecast</td>
<td>2061</td>
</tr>
<tr>
<td>Publish a forecast</td>
<td>2064</td>
</tr>
<tr>
<td>Capacity planning</td>
<td>2065</td>
</tr>
<tr>
<td>Getting started</td>
<td>2066</td>
</tr>
<tr>
<td>Create capacity planning scenarios</td>
<td>2066</td>
</tr>
<tr>
<td>Import estimated future shrinkage and available full-time employees</td>
<td>2068</td>
</tr>
<tr>
<td>Create capacity plans using forecasts and scenarios</td>
<td>2070</td>
</tr>
<tr>
<td>Review capacity plan output</td>
<td>2072</td>
</tr>
<tr>
<td>Override a capacity plan</td>
<td>2073</td>
</tr>
<tr>
<td>Re-run a capacity plan</td>
<td>2075</td>
</tr>
<tr>
<td>Download a capacity plan</td>
<td>2076</td>
</tr>
<tr>
<td>Publish a capacity plan</td>
<td>2077</td>
</tr>
<tr>
<td>Scheduling</td>
<td>2077</td>
</tr>
</tbody>
</table>
Getting started ................................................................. 2078
Scheduling roles: Who does what ........................................ 2078
Terminology ......................................................................... 2079
Create staff rules ................................................................. 2080
Create shift activities ........................................................... 2083
Create shift profiles ............................................................. 2085
Create staffing groups and rules ........................................... 2088
Generate, review, and publish a schedule ............................... 2091
How supervisors view published schedules ............................. 2096
How agents view their schedule ............................................. 2099
Add shift activities in draft or published schedules ................. 2100
Time off management .......................................................... 2105
Overtime management ......................................................... 2117
Voluntary time off management ............................................ 2120
Schedule Adherence ............................................................ 2123
Private optimization APIs ..................................................... 2128

**Voice ID** .......................................................................... 2130

- How Voice ID works .......................................................... 2130
  - Customer enrollment ....................................................... 2130
  - Customer authentication .................................................. 2131
- How much speech is needed for enrollment and authentication .................................................. 2131
- Batch enrollment ............................................................... 2131
- Known fraudster detection ................................................ 2132
  - Default watchlist .............................................................. 2132
- Voice spoofing detection .................................................... 2132
- What data is stored? ........................................................... 2133
- Voice ID domains ............................................................. 2133
  - Enrollment status ............................................................ 2134
  - Expired speakers ............................................................. 2135
  - Speaker and fraudster identifiers ...................................... 2135
- Enable Voice ID ............................................................... 2136
  - Before you begin ............................................................ 2136
  - Step 1: Read the BIPA Consent Acknowledgement ................ 2137
  - Step 2: Create a new Voice ID domain and encryption key .................................................. 2138
  - Step 3: Configure Voice ID in your flow ................................ 2141
- Assign permissions ........................................................... 2142
Search and review Voice ID results ................................................................. 2143
Voice ID results in a contact record ............................................................... 2144
Use the Voice ID APIs .................................................................................. 2145
Voice ID domain operations ......................................................................... 2145
Amazon Connect Integration Association APIs ............................................ 2146
Speaker, watchlist, and fraudster management APIs ..................................... 2147
Batch enrollment using audio data from prior calls ...................................... 2149
File schema for Speaker Enrollment Job ......................................................... 2150
Create and edit a fraudster watchlist .............................................................. 2153
File schema for Fraudster Registration Job .................................................... 2155
Amazon Connect Streams Voice ID APIs ....................................................... 2158
Voice ID event schema .................................................................................. 2158
Common fields in the event ......................................................................... 2158
Start Session Action .................................................................................... 2159
Update Session Action .................................................................................. 2160
Evaluate Session Action .............................................................................. 2161
Speaker Action .............................................................................................. 2162
Fraudster Action ............................................................................................ 2163
EnrollBySession ............................................................................................ 2163
StartSpeakerEnrollmentJob ......................................................................... 2164
StartFraudsterRegistrationJob ....................................................................... 2165
Security ......................................................................................................... 2167
Data protection ............................................................................................. 2168
Data handled by Amazon Connect ................................................................. 2169
Encryption at rest .......................................................................................... 2174
Encryption in transit ...................................................................................... 2187
Key management ............................................................................................ 2187
VPC endpoints (AWS PrivateLink) ................................................................. 2188
Identity and access management ................................................................... 2190
Audience ....................................................................................................... 2191
Authenticating with identities ....................................................................... 2191
Managing access using policies .................................................................... 2195
Required permissions for custom IAM policies ............................................ 2197
Restrict AWS resources that can be associated with Amazon Connect ............. 2224
How Amazon Connect works with IAM ....................................................... 2228
Identity-based policy examples ..................................................................... 2233
Resource-level policy examples ................................................................. 2244
AWS managed policies .................................................................................. 2252
Troubleshooting ............................................................................................. 2280
Use service-linked roles .................................................................................. 2281
Use service-linked roles for outbound campaigns ........................................... 2287
Using service-linked roles for Amazon AppIntegrations ................................. 2289
Using service-linked roles for Amazon Connect Customer Profiles ................. 2295
Using service-linked roles for Amazon Connect Managed Synchronization ..... 2299
Logging and monitoring ................................................................................ 2303
Tagging resources .......................................................................................... 2304
  Tag-based access control .............................................................................. 2306
Compliance validation .................................................................................... 2307
  Best practices for PII compliance ............................................................... 2308
  Best practices for PCI compliance ............................................................... 2308
  Best practices for HIPAA compliance ......................................................... 2309
Resilience ........................................................................................................ 2310
  Single-region telephony and softphone architecture .................................... 2310
  More resources ........................................................................................... 2311
Infrastructure security ..................................................................................... 2311
  Supported versions of TLS .......................................................................... 2311
  Other requirements ..................................................................................... 2312
Cross-service confused deputy prevention ..................................................... 2312
  Amazon Connect Customer Profiles .......................................................... 2313
  Amazon Connect Voice ID .......................................................................... 2315
  Amazon Connect chat message streaming cross-service confused deputy prevention .... 2316
Security Best Practices ................................................................................... 2317
  Amazon Connect Preventative Security Best Practices ................................. 2317
  Amazon Connect Detective Security Best Practices .................................... 2318
Agent training guide ....................................................................................... 2320
  Training video ............................................................................................ 2323
  Launch the CCP .......................................................................................... 2323
Log in and log out of CCP ............................................................................... 2324
  Problems logging in? .................................................................................. 2326
  Log out of CCP ........................................................................................... 2326
Allow access to cookies ................................................................................... 2327
  What happens if you don't choose Grant access when prompted? ............... 2328
Change your audio device settings ................................................................. 2329
  Change audio device settings in the CCP .................................................. 2330
  Prerequisite: Allow your browser to access your microphone ...................... 2331
  Firefox limitations ......................................................................................... 2331
  What to check when your audio device isn't working as expected .................. 2332
Forward calls to a mobile device ..................................................................... 2332
View your schedule ......................................................................................... 2333
Set your status to "Available" .......................................................................... 2334
Set your "Next status" ...................................................................................... 2334
  How to cancel "Next status" .......................................................................... 2335
  Set "Next status" while handling only ACW contacts ...................................... 2336
  Example 2: Set "Next status" while managing some chats on contact and other chats in ACW .......................................................... 2337
Work with calls in the CCP .............................................................................. 2338
  Accept incoming calls .................................................................................... 2338
  Transfer calls ................................................................................................. 2339
  Host multi-party calls ................................................................................... 2345
  Make outbound calls .................................................................................... 2350
  View a call transcript during ACW ............................................................... 2351
Work with chats ............................................................................................... 2352
  How to use the CCP to chat with contacts ................................................... 2353
  Search for quick responses in CCP .............................................................. 2358
  Transfer chats to another queue ..................................................................... 2360
  How to use the CCP to make a call while on a chat ...................................... 2362
Work with tasks ............................................................................................... 2367
  Accept a task ................................................................................................ 2367
  Create a new task .......................................................................................... 2370
  Transfer a task ............................................................................................... 2373
Use Customer Profiles .................................................................................. 2375
  Accept incoming contacts with Customer Profiles ....................................... 2377
  Create a new customer profile in the agent workspace ............................... 2385
  Search for a customer profile in the agent workspace .................................. 2388
Use Cases ........................................................................................................ 2390
  Search and view cases .................................................................................. 2391
  Add comments to a case .............................................................................. 2393
  Create a case ................................................................................................. 2394
Associate a contact with a case ................................................................. 2396
Edit a case ............................................................................................... 2396
Create a task from a case ......................................................................... 2397
Use Amazon Q in Connect ....................................................................... 2398
Search for content .................................................................................. 2399
Use real-time recommendations .............................................................. 2402
Use Voice ID ............................................................................................ 2403
Enroll a caller in Voice ID ......................................................................... 2404
Verification of an enrolled caller ............................................................... 2404
Caller has opted out .................................................................................. 2405
Authentication status = Not authenticated .............................................. 2405
Authentication status: Inconclusive ......................................................... 2406

Troubleshooting ...................................................................................... 2407
Use the Endpoint Test Utility .................................................................. 2407
Parameters to customize the Endpoint Test Utility .................................. 2408
Common Contact Control Panel (CCP) Issues ......................................... 2408
Download CCP logs ................................................................................ 2410
Troubleshooting Tools and Information .................................................. 2411
Gathering Helpful Information using the Streams API ............................ 2412
Analyzing the Data .................................................................................. 2413
Validation Testing .................................................................................... 2414
Mobile devices are not supported ........................................................... 2417
Can't make outbound calls ...................................................................... 2417
Attachments are not appearing ............................................................... 2418
Internal firewall settings are preventing access ...................................... 2418
Attachments are too large, too many, or don't meet file type requirements 2418
Humming sound in headset ...................................................................... 2419
Verify Firefox sample rate ....................................................................... 2419
Verify Chrome sample rate ..................................................................... 2419
One-way audio from customers? .............................................................. 2422

Release notes ......................................................................................... 2423
December 2023 Updates ......................................................................... 2423
Contacts Answered/Abandoned in X ......................................................... 2423
November 2023 Updates ......................................................................... 2423
Customer Profiles provides a generative AI powered customer data mapping capability . 2423
No-code UI builder for step-by-step guides .............................................. 2423
Added Amazon Q in Connect ........................................................................................................... 2423
Amazon Connect Contact Lens provides real-time conversational analytics for chat ........ 2424
Amazon Connect Contact Lens provides generative AI–powered contact summarization (Preview) ........................................................................................................................................ 2424
Amazon Connect supports in-app, web, and video calling ......................................................... 2425
Amazon Connect supports two-way SMS .................................................................................... 2425
Analytics data lake (Preview) ....................................................................................................... 2425
Added metrics to the GetMetricDataV2 action ........................................................................... 2426
Customer Profiles block enhancements ....................................................................................... 2426
View and manage applied service quotas for Amazon Connect using AWS Service Quotas ........................................................................................................................................... 2426
Added an action to AmazonConnectServiceLinkedRolePolicy ................................................ 2426
Amazon Connect now provides a Contact Lens conversational analytics dashboard .......... 2426
Amazon Connect now provides a pre-built queue performance dashboard ............................. 2427
Amazon Connect prompts configuration page provides CloudTrail coverage ....................... 2427
Amazon Connect enables integration with your preferred file scanning application to detect malware ........................................................................................................................................... 2427
Amazon Connect outbound campaigns voice dialing API ......................................................... 2427
Amazon Connect Cases supports author name on comments .................................................. 2428
Updated AmazonConnectCampaignsServiceLinkedRolePolicy service-linked role managed policy ........................................................................................................................................... 2428
Added Create persistent chat association flow block and
CreatePersistentContactAssociation API ..................................................................................... 2428
Optimization to how the CCP detects and handles stale WebSocket connections .................. 2428
Added new service-linked role policy and service-linked role .................................................. 2428
Added Contact Lens conversational analytics metrics to the GetMetricDataV2 API ............. 2429
Added configuration management across AWS Regions for Amazon Connect Global Resiliency customers ........................................................................................................................................... 2429
October 2023 Updates .................................................................................................................. 2429
Added actions to AmazonConnectServiceLinkedRolePolicy ................................................ 2429
Third-party applications preview ................................................................................................. 2429
Added actions to AmazonConnectServiceLinkedRolePolicy ................................................ 2430
Added the UpdatePhoneNumberMetadata API ............................................................................ 2430
Add as many as four access control tags to a single security profile ....................................... 2430
Added actions to AmazonConnectServiceLinkedRolePolicy ................................................ 2430
CTI Adapter upgrade for third-party cookies .............................................................................. 2430
Create and customize up to 15 communications widgets ........................................... 2431
Access the trailing 90 days of historical agent and contact metrics ............................. 2431
Added actions to AmazonConnectServiceLinkedRolePolicy ..................................... 2431

September 2023 Updates ........................................................................................................... 2432
Released Amazon Connect Client Application v1.0.2.38 .................................................. 2432
Added "View my contacts" permission .............................................................................. 2432
Streams API upgrade for third-party cookies .................................................................... 2432
Create alerts on real-time metrics ....................................................................................... 2432
"Maximum contacts in queue" includes all channels ......................................................... 2432
Manage contacts from the Contact details page .............................................................. 2433
Upload file attachments to cases ....................................................................................... 2433
Search for in-progress contacts .......................................................................................... 2433
Subscribe to the Contact Data Updated event in the contact event stream ................... 2433
APIs to programmatically configure views in step-by-step guides .................................... 2433
Support for UIFN in more than 60 countries ..................................................................... 2433

August 2023 Updates ............................................................................................................. 2434
Voice dialing for outbound campaigns, no agents required .............................................. 2434
Amazon Connect Cases supports nine additional languages ........................................... 2434
Granular access controls using resource tags for the agent activity audit report .......... 2434
Enhanced user bulk edit ....................................................................................................... 2434
Amazon Connect scheduling supports agent group activities .......................................... 2434
GA for global sign-in and agent distribution capabilities .................................................. 2435
100 rows on real-time metrics tables .............................................................................. 2435
Sorting on column header names ....................................................................................... 2436
Route based on time since last inbound contact ................................................................ 2436

July 2023 Updates .................................................................................................................. 2436
Customize the names of flow blocks ................................................................................... 2436
Archive, restore, and delete flows and modules ............................................................... 2436
Undo and redo actions in the flow designer ....................................................................... 2437
Add notes to a flow block .................................................................................................... 2437
Use the mini-map to navigate a flow .................................................................................. 2438
Restrict attributes to specific flows .................................................................................... 2438
Import time off balances ..................................................................................................... 2438
Schedule flexible days and shift activities based on shift length .................................... 2439
Amazon Connect Customer Profiles supports rule-based matching and merging ............ 2439
Released Amazon Connect Client Application v1.0.1.33 .................................................. 2439
Amazon Connect Cases provides case assignment ........................................ 2439
Contact Lens Conversational Analytics metrics in the API .......................... 2440
Amazon Connect Wisdom supports real-time recommendations for chat conversations .......................... 2440
Delete queues and routing profiles programmatically .................................. 2440
June 2023 Updates ...................................................................................... 2441
Agents can change their audio device settings in the CCP and agent workspace .......................... 2441
Amazon Connect Chat: New interactive message types ................................ 2441
GetMetricDataV2 API: Region availability and new functionality .................. 2441
Search for existing tags within an Amazon Connect instance ......................... 2441
Added screen recording capabilities to Contact Lens .................................... 2442
Amazon Connect scheduling allows agents to manage time off requests ........ 2442
Real-time data export of unified customer profiles to an Amazon Kinesis Data Stream ... 2442
May 2023 Updates ...................................................................................... 2442
Added theme detection to Contact Lens ......................................................... 2442
New APIs for managing prompts .................................................................. 2442
Added supervisor alerts on agent performance ............................................. 2443
Interactive messages: Rich formatting in chat titles and subtitles .................... 2443
April 2023 Updates ..................................................................................... 2443
GA for Amazon Connect evaluation capabilities ........................................... 2443
New API: Use CreateParticipant to customize chat flow experiences .......... 2443
Customer Profiles displays case information in the agent workspace .......... 2444
Added Cross-channel concurrency ............................................................... 2444
Set Voice ID block supports fraud watchlist ID ............................................. 2444
Search, sort, and filter published agent schedules .......................................... 2444
March 2023 Updates ................................................................................... 2444
Added Wisdom support for Microsoft SharePoint Online ............................. 2444
Create step-by-step guides for your agents .................................................. 2445
Added support for nested JSON in Invoke AWS Lambda function flow block .... 2445
Added Show View flow block ...................................................................... 2445
Added staff level shift profile ...................................................................... 2445
Added support for multiple fraudster watchlists .......................................... 2445
Search and sort schedules in the Schedule Manager ...................................... 2445
Added the ability to configure multiple IAM roles that can be assigned to a single user when using SAML 2.0 ................................................................. 2446
Added panel template for interactive chat messages ...................................... 2446
Added GetMetricDataV2 API ..................................................................... 2446
February 2023 Updates

- Added new attribute type ENHANCED_CONTACT_MONITORING to Describe, List and Update Instance Attribute APIs
- Added the DeleteDomain API for Cases
- Added RelatedContactId to StartTaskContact API
- Amazon Connect Cases integrates with AWS PrivateLink
- Added support for more granular access controls (using resource tags) to view real-time metrics for agents, queues, and routing profiles
- Added support to provide more granular permissions to metrics reports, including new permissions for real-time metrics, historical metrics, and agent activity audit
- Added support to provide visibility into an agent’s next activity
- Apply S3 Object Lock for the call recordings bucket
- CloudFormation templates for instance management

January 2023 Updates

- Added long lasting, persistent chat experiences

December 2022 Updates

- Added message receipts feature for chat messages
- Updates to GetCurrentMetricData and GetCurrentUserData
- Added chat timeouts for chat participants
- Microsoft Edge Chromium support
- Amazon Connect supports JSON as a content type for chat messages
- Added topic on Amazon Connect availability by Region
- Contact Lens granular data redaction
- Additional Contact Lens language support and Region availability
- Released Barge to allow contact center managers to join ongoing calls
- Added user hierarchy to bulk user upload
- Granular access controls using resource tags for users, security profiles, routing profiles, and queues
- Bulk user import now includes agent hierarchy and tags
- Released Rules Function language
- GA for Rules APIs
- Search contacts by agent’s first or last name is available in AWS GovCloud

November 2022 Updates

- Create step-by-step guides for your agents
- GA for Forecasting, capacity planning, and scheduling
- Released Contact Lens evaluation forms for preview
Released Contact Lens conversational analytics capabilities for Amazon Connect chat .... 2451
Added configurable Lex timeouts in chat .......................................................... 2452
Create rules that send email notifications ....................................................... 2452
Added MonitorContact API ........................................................................... 2452
Manage saved reports (admin) ........................................................................ 2452
Search for profiles using multiple search keys ............................................... 2452
Delete quick connects using the Amazon Connect console ......................... 2453
Added DismissUserContact API ................................................................. 2453
October 2022 Updates ..................................................................................... 2453
Add secondary email address and mobile number to user accounts .......... 2453
Emojis for chat messages ............................................................................... 2453
Released support for Enhanced 911 (E911) ............................................... 2453
GA for Amazon Connect Global Resiliency .................................................... 2453
Added Ctrl+Shift+F to search flow block titles and metadata .................. 2454
Released Amazon Connect Cases for General Availability ................. 2454
September 2022 Updates ............................................................................... 2455
Searching for a contact? Choose from a list of categories .................... 2455
Updated flow designer .................................................................................... 2455
Search for Amazon Connect users by first name, last name, login, and more 2461
Queue dashboard ............................................................................................. 2462
August 2022 Updates ...................................................................................... 2462
Contact search: Apply "Match any" or "Match all" to Contact Lens category searches .... 2462
Evaluate calls for voice spoofing .................................................................... 2462
......................................................................................................................... 2462
July 2022 Updates ............................................................................................ 2462
Released updates for rich text format rendering .......................................... 2464
View call transcript using the CCP or agent application ......................... 2464
June 2022 Updates ........................................................................................... 2465
Support for Lex intent confidence scores and sentiment analysis ............ 2465
Metrics Updates .............................................................................................. 2465
......................................................................................................................... 2466
New contact transferred related metrics ....................................................... 2467
Changes to real-time metrics agent tables ............................................... 2467
Faster reload times for the Real-time metrics page .................................... 2468
Released Amazon Connect Cases (Preview) .......................................................... 2468
GA for Amazon Connect outbound campaigns .................................................... 2468
Released GetCurrentUserData API ..................................................................... 2468
Released task templates ..................................................................................... 2468
New API to transfer contacts ............................................................................. 2468
May 2022 Updates ................................................................................................. 2469
  Updated workflow for outbound campaigns ...................................................... 2469
  Voice ID expires speakers ............................................................................... 2469
April 2022 Updates ............................................................................................... 2469
  New API to change an agent's current status ..................................................... 2469
  New API to search for users by name, agent hierarchies, and tags ..................... 2469
  New APIs to claim and configure phone numbers .......................................... 2469
  Multi-party calls ............................................................................................... 2470
  Play prompts from an S3 bucket ...................................................................... 2472
  CloudTrail support for queues and routing profiles ....................................... 2472
March 2022 Updates ............................................................................................. 2473
  Rich messaging for chat ................................................................................... 2473
  Customer Profiles: Object type mapping user interface .................................... 2473
February 2022 Updates ......................................................................................... 2473
  Added bulk ingestion of data for Customer Profiles ....................................... 2473
  New CloudWatch metrics for chat .................................................................... 2473
January 2022 Updates ........................................................................................ 2473
  Configure maximum chat duration up to 7 days ............................................. 2473
  Add custom vocabularies to Contact Lens ....................................................... 2473
Earlier Updates .................................................................................................. 2474
December 2021 Updates ..................................................................................... 2474
November 2021 Updates .................................................................................... 2474
October 2021 Updates ....................................................................................... 2476
September 2021 Updates .................................................................................... 2477
August 2021 Updates ......................................................................................... 2478
July 2021 Updates ............................................................................................... 2478
June 2021 Updates .............................................................................................. 2482
May 2021 Updates ............................................................................................... 2483
April 2021 Updates .............................................................................................. 2484
March 2021 Updates ............................................................................................ 2485
February 2021 Updates ........................................................................................ 2488
January 2021 Updates .......................................................................................................................... 2493
December 2020 Updates .......................................................................................................................... 2494
November 2020 Updates ......................................................................................................................... 2496
October 2020 Updates ............................................................................................................................. 2497
September 2020 Updates ......................................................................................................................... 2498
August 2020 Updates ............................................................................................................................... 2499
July 2020 Updates ..................................................................................................................................... 2500
June 2020 Updates ................................................................................................................................. 2501
May 2020 Update ..................................................................................................................................... 2505
April 2020 Update .................................................................................................................................... 2505
March 2020 Update .................................................................................................................................. 2506
February 2020 Update .............................................................................................................................. 2506
January 2020 Update ............................................................................................................................... 2506
December 2019 Update ............................................................................................................................ 2507
November 2019 Update ........................................................................................................................... 2507
October 2019 Update ............................................................................................................................... 2513
June 2019 Update .................................................................................................................................... 2514
May 2019 Updates .................................................................................................................................... 2514
April 2019 Updates .................................................................................................................................... 2514
March 2019 Update ................................................................................................................................... 2515
February 2019 Updates ............................................................................................................................ 2515
January 2019 Updates ............................................................................................................................... 2516
December 2018 Updates ............................................................................................................................ 2517
November 2018 Updates ........................................................................................................................... 2518
October 2018 Updates .............................................................................................................................. 2519
September 2018 Updates .......................................................................................................................... 2520
August 2018 Updates ............................................................................................................................... 2520
July 2018 Updates ..................................................................................................................................... 2521
June 2018 Updates ................................................................................................................................... 2522
April and May 2018 Updates ...................................................................................................................... 2523
Document history ....................................................................................................................................... 2525
Earlier updates ........................................................................................................................................... 2621

Glossary .................................................................................................................................................... 2630
 Channel .................................................................................................................................................. 2630
 Contact attribute ................................................................................................................................... 2630
 Flow ...................................................................................................................................................... 2630
Instance ..................................................................................................................... 2630
Letter of Authorization ........................................................................................................... 2630
Losing carrier ............................................................................................................................ 2631
Mutually agreed date and time .............................................................................................. 2631
Omnichannel ............................................................................................................................. 2631
Phone number portability ........................................................................................................... 2631
Queue ........................................................................................................................................ 2631
Winning carrier ........................................................................................................................ 2631
Amazon Connect is an omnichannel cloud contact center. You can set up a contact center in a few steps, add agents who are located anywhere, and start engaging with your customers.

You can create personalized experiences for your customers using omnichannel communications. For example, you can **dynamically offer chat and voice contact**, based on such factors as customer preference and estimated wait times. Agents, meanwhile, conveniently handle all customers from just **one interface**. For example, they can chat with customers, and create or respond to tasks as they are routed to them.

Amazon Connect is an open platform that you can integrate with other enterprise applications, such as **Salesforce**. You can use Amazon Connect with other AWS services to provide innovative new experiences for your customers.

### How to get started

If you are a first-time user of Amazon Connect, we recommend that you do the following:

- Read about the **concepts**
- Read the **architectural guidance**
- **Set up your contact center**

### Pricing

With Amazon Connect, you pay only for what you use. For more information, see [Amazon Connect pricing](#).
The power of AWS with Amazon Connect

To help provide a better contact center, you can use Amazon Connect with the following AWS services.

### Development

You can use AWS Lambda functions to either look up or post data to sources outside of Amazon Connect. For example, you can look up an inbound caller on Salesforce based on the customer’s phone number. The function may return such results as the customer name, membership level (for example, frequent flyer), last order, and order status. Then based on that information, the call can be routed to an Amazon Lex bot or an agent.

You can also use Lambda with AWS databases like DynamoDB to create dynamic routing abilities. For example, you can retrieve a prompt in a specific language, based on input from the customer.

API Gateway and Step Functions further enhance the abilities of Lambda.

For more information, see:

- [Invoke AWS Lambda functions](#)
Storage

Amazon Connect uses Amazon Simple Storage Service (Amazon S3) to store recorded conversations and exported reports. When you set up Amazon Connect, it creates default buckets for these requirements, or you can point it to existing Amazon S3 infrastructure. For more information, see Step 4: Data storage in Create an Amazon Connect instance.

VPC endpoints are not supported.

You can also manage the Amazon S3 policies to move data to Amazon S3 Glacier for less expensive long-term storage. However, it breaks the link in the contact record in Amazon Connect. To fix this, use a Lambda function to rename the S3 Glacier object to match the data in the contact record.

Database

You can use AWS databases with Amazon Connect for a variety of reasons. For example, with DynamoDB, you can create quick tables of data.

You can also create tables of dynamic information for call routing. For example, a Lambda function can write inbound calls to a DynamoDB table, then query the table to see if there are other matches for the phone number. If so, a decision can be made to send the caller to the same queue as before, or to flag them as a repeat caller.

For more information, see:

- Blog post: Creating dynamic, personalized experiences in Amazon Connect

Analytics

Amazon Connect tracks all interactions using contact records. Contact records are used for real-time and historical metrics reports. You can also use Amazon Kinesis to stream them to an AWS database like Amazon Redshift or Amazon Athena for BI analysis (Amazon QuickSight, or a third party such as Tableau). There are AWS CloudFormation templates available to set up this functionality for Amazon Redshift and Athena.

To perform analysis on your flow logs, you can set up an Amazon Kinesis stream to stream your flow log data from CloudWatch to a data warehouse service, such as Amazon Redshift. You can combine the flow log data with other Amazon Connect data in your warehouse, or run queries to identify trends or common issues with a flow.
For more information, see:

- How to access Kinesis Video Streams data
- Blog post: Recovering abandoned calls with Amazon Connect

### Machine Learning (ML) and Artificial Intelligence (AI)

Amazon Connect uses the following services for ML/AI:

- Amazon Lex—Lets you create a chatbot to use as Interactive Voice Response (IVR). For more information, see Add an Amazon Lex bot to Amazon Connect.
- Amazon Polly—Provides text-to-speech in all flows. For more information, see Add text-to-speech to prompts and SSML tags supported by Amazon Connect.
- Amazon Transcribe—Grabs conversation recordings from Amazon S3, and transcribes them to text so you can review them.
- Amazon Comprehend—Takes the transcription of recordings, and applies speech analytics machine learning to the call to identify sentiment, keywords, adherence to company policies, and more.

### Messaging

Amazon Connect uses the following services for messaging:

- Amazon Pinpoint—Use as an outbound messaging trigger for events; for example, bulk messaging (such as outbound marketing campaigns). For more information, see this blog post: Using Amazon Pinpoint to send text messages in Amazon Connect.
- Amazon Simple Notification Service (Amazon SNS)—Use to send and receive SMS and other channel notifications. Amazon SNS is particularly useful for sending alerts and validations.
- Amazon Simple Email Service (Amazon SES)—Use to send validation e-mails, such as a password reset bot sending a confirmation of the transaction.

### Security

Amazon Connect uses the following services for added security:
• AWS Identity and Access Management (IAM)—Use to manage permissions for users. Amazon Connect users require permission for services. For more information, see **Identity and access management for Amazon Connect**.

• AWS Directory Service—Amazon Connect supports user federation through the internal directory (created in the Amazon Connect instance), using Active Directory integration (MAD, ADFS) or SAML 2.0.

For more information, see:

• **Plan your identity management in Amazon Connect**

• Blog post: **Enabling federation with AWS Single Sign-On and Amazon Connect**

**Management**

Amazon Connect uses the following services for monitoring usage:

• Amazon CloudWatch—Collects logs, service metrics, performance metrics for Amazon Connect. For more information, see **Monitoring your instance using CloudWatch**.

• AWS CloudTrail—Provides a record of Amazon Connect API calls.

For more information about Amazon Connect and AWS CloudTrail, see **Logging Amazon Connect API calls with AWS CloudTrail**.

• AWS CloudFormation—Amazon Connect supports using AWS CloudFormation for initiating an instance with all the supported channels enabled. For more information, see **AWS::Connect::Instance**.

**Availability of Amazon Connect services by Region**

This topic lists the AWS Regions where Amazon Connect services are available.

**Contents**

• **Amazon Connect availability by Region**

• **AppIntegrations availability by Region**

• **Amazon Q in Connect**

• **Cases availability by Region**

• **Contact Lens availability by Region**
• Customer Profiles availability by Region
• Voice ID availability by Region
• Agent workspace (step-by-step guides)
• Agent workspace third-party applications (Preview)
• Chat messaging: SMS subtype
• Communications widget
• In-app, web, and video calling capabilities
• Forecasting, capacity planning, and scheduling
• Live media streaming
• Outbound campaigns
• Tasks

Amazon Connect availability by Region

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>connect.us-east-1.amazonaws.com&lt;br&gt;connect-fips.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>connect.us-west-2.amazonaws.com&lt;br&gt;connect-fips.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>connect.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>connect.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-southeast-1</td>
<td>connect.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region Name</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>(Singapore)</td>
<td>ap-southeast-2</td>
<td>connect.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>connect.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>connect.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>connect.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>connect.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>connect.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td>us-gov-west-1</td>
<td>connect.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**AppIntegrations availability by Region**

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region Name</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>app-integrations.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app-integrations-fips.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

AppIntegrations
<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>app-integrations.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app-integrations-fips.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>app-integrations.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>app-integrations.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>app-integrations.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>app-integrations.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>app-integrations.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>app-integrations.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>app-integrations-fips.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>app-integrations.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>
### Amazon Connect

#### Region Name | Region | Endpoint | Protocol
--- | --- | --- | ---
Europe (London) | eu-west-2 | app-integrations.eu-west-2.amazonaws.com | HTTPS

#### Amazon Q in Connect

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Europe (Frankfurt)
- Europe (London)

#### Cases availability by Region

#### Region Name | Region | Endpoint | Protocol
--- | --- | --- | ---
US East (N. Virginia) | us-east-1 | cases.us-east-1.amazonaws.com | HTTPS
cases-fips.us-east-1.amazonaws.com | HTTPS
US West (Oregon) | us-west-2 | cases.us-west-2.amazonaws.com | HTTPS
cases-fips.us-west-2.amazonaws.com | HTTPS
Asia Pacific (Singapore) | ap-southeast-1 | cases.ap-southeast-1.amazonaws.com | HTTPS
<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>cases.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>cases.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>cases.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>cases.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**Contact Lens availability by Region**

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>contact-lens.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>contact-lens.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>contact-lens.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>contact-lens.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>contact-lens.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>contact-lens.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>contact-lens.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>contact-lens.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>contact-lens.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**Contact Lens features by Region**

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact search</th>
<th>Screen recording</th>
<th>Evaluation capabilities</th>
<th>Post-call analytics</th>
<th>Post-chat analytics</th>
<th>Real-time call analytics</th>
<th>Theme detection</th>
<th>Extended language support</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Region</td>
<td>Contact search</td>
<td>Screen recording</td>
<td>Evaluation capabilities</td>
<td>Post-call analytics</td>
<td>Post-chat analytics</td>
<td>Real-time call analytics</td>
<td>Theme detection</td>
<td>Extended language support</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Customer Profiles availability by Region

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>profile.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile-fips.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>profile.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile-fips.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>profile.af-south-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>profile.ap-northeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>profile.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-southeast-2</td>
<td>profile.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>(Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-northeast-1</td>
<td>profile.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>(Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>profile.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile-fips.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>profile.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>profile.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**Voice ID availability by Region**

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>voiceid.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voiceid-fips.us-east-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>voiceid.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voiceid-fips.us-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-southeast-1</td>
<td>voiceid.ap-southeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region</td>
<td>Endpoint</td>
<td>Protocol</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>(Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-southeast-2</td>
<td>voiceid.ap-southeast-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>(Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>ap-northeast-1</td>
<td>voiceid.ap-northeast-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>(Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada Central</td>
<td>ca-central-1</td>
<td>voiceid.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voiceid-fips.ca-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe Frankfurt</td>
<td>eu-central-1</td>
<td>voiceid.eu-central-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Europe London</td>
<td>eu-west-2</td>
<td>voiceid.eu-west-2.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**Agent workspace (step-by-step guides)**

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (London)
• AWS GovCloud (US-West)

Agent workspace third-party applications (Preview)

• US East (N. Virginia)
• US West (Oregon)
• Asia Pacific (Sydney)
• Europe (London)

Chat messaging: SMS subtype

• US East (N. Virginia)
• US West (Oregon)
• Asia Pacific (Singapore)
• Asia Pacific (Tokyo)
• Canada (Central)
• Europe (Frankfurt)
• Europe (London)

Communications widget

• US East (N. Virginia)
• US West (Oregon)
• Asia Pacific (Seoul)
• Asia Pacific (Singapore)
• Asia Pacific (Sydney)
• Asia Pacific (Tokyo)
• Canada (Central)
• Europe (Frankfurt)
• Europe (London)
In-app, web, and video calling capabilities

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (London)

Forecasting, capacity planning, and scheduling

- US East (N. Virginia)
- US West (Oregon)
- Canada (Central)
- Asia Pacific (Sydney)
- Europe (London)

Live media streaming

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
Outbound campaigns

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Sydney)
- Canada (Central)
- Europe (Frankfurt)
- Europe (London)

The phone numbers that outbound campaigns can call are based on the AWS Region where your Amazon Connect instance is created.

- From instances created in US East (N. Virginia) or US West (Oregon) you can call all phone numbers based in the US.
- From instances created in Canada (Central) you can call all phone numbers based in Canada.
- From instances created in Asia Pacific (Sydney) you can call phone numbers based in Australia and New Zealand. There are a few specific restrictions explained in [Make predictive and progressive calls using Amazon Connect outbound campaigns](#).
- From instances created in Europe (Frankfurt) or Europe (London) you can call all phone numbers based in the UK, Italy, or Spain.
- No other combinations are supported. For example, you can't make campaign calls from Europe (London) to US phone numbers, or from Europe (Frankfurt) to New Zealand phone numbers.

Tasks

- US East (N. Virginia)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
Before you work with Amazon Connect, verify that your browser is supported using the following table.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>How to check your version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest three versions</td>
<td>Open Chrome and type chrome://version in your address bar. The version is in the Google Chrome field at the top of the results.</td>
</tr>
<tr>
<td>Microsoft Edge Chromium</td>
<td>Latest three versions</td>
<td>Open Edge. On the menu, choose Help and feedback and then choose About Microsoft Edge. The version number is listed in the About section.</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Latest three versions</td>
<td>Open Firefox. On the menu, choose the Help icon and</td>
</tr>
</tbody>
</table>

⚠️ Important

If you found this page because you need to contact Amazon for support, see Amazon Customer Service (Amazon orders and deliveries) or AWS Support (Amazon Web Services) instead.
## Browsers on mobile devices

The Amazon Connect console, Contact Control Panel (CCP), and agent workspace do not support mobile browsers. However, your agents can forward the audio portion of the call to their mobile device. For instructions, see [Forward calls to a mobile device (iPhone, Android)].

### Supported browsers and mobile OS for in-app, web, and video calling capabilities

- Amazon Chime SDK for iOS and Android:
  - iOS version 13 and later
  - Android OS version 8.1 and later, ARM and ARM64 architecture
- Web browsers for out-of-the-box communications widget and JS SDK
  - Latest three versions of Google Chrome, Firefox, Safari, and Microsoft Edge Chromium on MacOS, Windows, iOS, and Android.

For more information, see [Set up in-app, web, and video calling capabilities].

The communications widget supports browser notifications for desktop devices. For more information, see [Browser notifications].

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>How to check your version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox ESR</td>
<td>Versions are supported until their Firefox end-of-life date. For details, see the Firefox ESR release calendar.</td>
<td>Open Firefox. On the menu, choose the Help icon and then choose About Firefox. The version number is listed under the Firefox name.</td>
</tr>
</tbody>
</table>
Issue with Firefox version 86

The following issue may occur if you embed the Amazon Connect Contact Control Panel (CCP) into your agent application and your users access the Amazon Connect CCP using the Firefox web browser with Enhanced Tracking Protection browser setting set to Strict.

An upgrade to Firefox, specifically Firefox non-ESR version 86 released on February 23, 2021, introduced Total Cookie Protection which modified cookie sharing behavior across sites for users with Enhanced Tracking Protection set to Strict (Firefox defaults to Standard). Users with this specific browser setting and version combination may be unable to access the Amazon Connect CCP when embedded in another application, preventing them from handling contacts.

To prevent impact to your users (agents), we recommend that your users do one of the following:

- Confirm (or set) Enhanced Tracking Protection as Standard in their browser settings. Users can do this by following instructions documented here.
- Do not upgrade their Firefox browser version to v86 or higher.
- Use Google Chrome or Microsoft Edge to access the Amazon Connect CCP.

Supported screen readers

You can use the following screen readers with the latest version of the Amazon Connect Contact Control Panel (the CCP URL ends with /ccp-v2):

- JAWS
- NVDA
- VoiceOver

Languages supported by Amazon Connect

This topic lists Amazon Connect features and which languages they support.
• Amazon Connect Cases
• Amazon Connect Contact Lens
• Pattern match languages
• Amazon Connect forecasting, capacity planning, and scheduling
• Amazon Q in Connect
• Amazon Lex
• Amazon Polly

Contact Control Panel

<table>
<thead>
<tr>
<th>CCP</th>
<th>Supported languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Control Panel - latest version</td>
<td>• Chinese (Simplified)</td>
</tr>
<tr>
<td></td>
<td>• Chinese (Traditional)</td>
</tr>
<tr>
<td></td>
<td>• English</td>
</tr>
<tr>
<td></td>
<td>• French</td>
</tr>
<tr>
<td></td>
<td>• German</td>
</tr>
<tr>
<td></td>
<td>• Italian</td>
</tr>
<tr>
<td></td>
<td>• Japanese</td>
</tr>
<tr>
<td></td>
<td>• Korean</td>
</tr>
<tr>
<td></td>
<td>• Portuguese (Brazilian)</td>
</tr>
<tr>
<td></td>
<td>• Spanish</td>
</tr>
</tbody>
</table>

| Contact Control Panel - earlier version | English                                      |
|                                        | French                                       |
|                                        | German                                       |
|                                        | Italian                                      |
|                                        | Japanese                                     |
|                                        | Korean                                       |
|                                        | Portuguese (Brazilian)                       |
|                                        | Spanish                                      |
Chat message content

Amazon Connect provides full Unicode support. You can chat with customers in any language of your choice.

Amazon Connect admin website

• Chinese (Simplified)
• Chinese (Traditional)
• English
• French
• German
• Italian
• Japanese
• Korean
• Portuguese (Brazilian)
• Spanish

Amazon Connect Cases

• Chinese (Simplified)
• Chinese (Traditional)
• English
• French
• German
• Italian
• Japanese
• Korean
• Portuguese (Brazilian)
• Spanish
## Amazon Connect Contact Lens

<table>
<thead>
<tr>
<th>Languages</th>
<th>Post-call/chat analytics</th>
<th>Post-call/chat redaction</th>
<th>Real-time call analytics</th>
<th>Real-time redaction</th>
<th>Key highlights</th>
<th>Theme detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic (Gulf)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>English (Australia)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (Great Britain)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (New Zealand)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (South Africa)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (United States)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (India)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>English (Ireland)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>English (Scotland)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>English (Wales)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Languages</td>
<td>Post-call/chat analytics</td>
<td>Post-call/chat redaction</td>
<td>Real-time call analytics</td>
<td>Real-time redaction</td>
<td>Key highlights</td>
<td>Theme detection</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>French (Canada)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>French (France)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Germany)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>German (Switzerland)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hindi (India)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italian (Italy)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japanese (Japan)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korean (South Korea)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mandarin (Mainland China)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portuguese (Brazil)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Languages</td>
<td>Post-call/chat analytics</td>
<td>Post-call/chat redaction</td>
<td>Real-time call analytics</td>
<td>Real-time redaction</td>
<td>Key highlights</td>
<td>Theme detection</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Portuguese (Portugal)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish (Spain)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish (United States)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Pattern match languages**

In Contact Lens, the pattern match feature supports the following languages:

- English (United States)
- Arabic (Gulf)
- Chinese
- German (Germany)
- French (France)
- Hindi (Indian)
- Italian
- Japanese
- Korean
- Portuguese
- Spanish (Spain)

**Amazon Connect forecasting, capacity planning, and scheduling**

- English (United States)
Amazon Q in Connect

- English (Australia)
- English (Great Britain)
- English (United States)

Amazon Lex

See Languages and locales supported by Amazon Lex V2 in the Amazon Lex V2 Developer's Guide.

Amazon Polly

See Voices in Amazon Polly in the Amazon Polly Developer Guide.

Amazon Connect service quotas

All service quotas can be adjusted/increased unless otherwise noted.

Your AWS account has default quotas, formerly referred to as limits, for each AWS service.

To request a quota increase, see Requesting a quota increase in the Service Quotas User Guide. If the quota is not yet available in Service Quotas, use the Amazon Connect service quotas increase form. You must be signed in to your AWS account to access the form.

Contents

- Important things to know
- Amazon Connect quotas
- Amazon Connect AppIntegrations service quotas
- Amazon Q in Connect service quotas
- Amazon Connect Cases service quotas
- Contact Lens service quotas
- Amazon Connect Customer Profiles service quotas
- Amazon Connect Outbound campaigns service quotas
- Amazon Connect Voice ID service quotas
- How contacts are counted
- Amazon Connect feature specifications
• Countries you can call by default

• API throttling quotas

Important things to know

• You must create your instance before you can request a service quota increase.

• We review each request for a quota increase. For smaller increase requests, we can approve in hours. Larger increase requests take time to review, process, approve, and deploy. Depending on your specific implementation, your resource, and the size of quota that you want, a request can take up to 3 weeks. An extra-large worldwide increase can potentially take months. If you're increasing your quotas as part of a larger project, keep this information in mind and plan accordingly.

• Use the same form to submit a request to port your US phone number from your current carrier to Amazon Connect. For more information about porting phone numbers, see Port your current phone number to Amazon Connect.

• The quotas apply per AWS Region. You can have multiple Amazon Connect instances in each Region. It's possible to raise quotas for all instances in a Region.

• Default quota values in this documentation are specifically for new accounts. Because quotas defaults have been adjusted over time, the default and applied quota values for your account might be lower than the default values described below.

• Not all quotas can be adjusted.

• There are two types of quota adjustability: account level and resource-level.

  • Account level quotas, when adjusted, will apply to all Amazon Connect instances in this account and region. For example, the maximum transactions per second (TPS) limits for a specific API.

  • Resource level quotas, when adjusted, will only apply to resources within a specific Amazon Connect instance. For example, the maximum number of users per instance. Resource level quotas cannot be adjusted at the account level.

⚠️ Important

You need AWS CLI version 2.13.20 or higher to view and manage resource-level quotas such as Phone numbers per instance for Amazon Connect.
### Amazon Connect quotas

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
<th>Adjustability</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lambda functions per instance</td>
<td>50</td>
<td>No</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Agent status per instance</td>
<td>50</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td>Amazon Connect instances per account</td>
<td>2</td>
<td>Yes</td>
<td>Account Level</td>
</tr>
<tr>
<td>Amazon Lex bots per instance</td>
<td>70</td>
<td>No</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Amazon Lex V2 bot aliases per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Concurrent active calls per instance</td>
<td>10</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>For more information, see the section called &quot;How contacts are counted&quot;.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent active chats per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>This includes chats that are waiting and SMS.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If this quota is exceeded, the API call fails with a quota exceeded error.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Default</td>
<td>Adjustable</td>
<td>Adjustability</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Concurrent active tasks per instance</td>
<td>2500 concurrent active tasks</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td>All tasks that have not yet ended are considered active and are counted as concurrent tasks: tasks that are being routed in flows, waiting in a queue for an agent, being handled by agents, or being run in After Contact Work (ACW).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flows per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Hours of operation per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Maximum duration that a task can be scheduled in future</td>
<td>6 days</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td>Maximum number of reschedules allowed for a task scheduled for a future time</td>
<td>20</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td>Modules per instance</td>
<td>200</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td>Name</td>
<td>Default</td>
<td>Adjustable</td>
<td>Adjustability</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Phone numbers per instance</td>
<td>5</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It's possible to get an error message that &quot;You've reached the limit of Phone Numbers,&quot; even if it's the first time you've claimed a phone number. All the issues that cause this error message require help from AWS Support to resolve.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prompt per instance</td>
<td>500</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Queues per instance</td>
<td>50</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Queues per routing profile per instance</td>
<td>50</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>This quota refers to number of queue/channel combinations per routing profile. For example, in the following image there are two queues, but there are three queue-channel combinations: Escalation queue Voice, Escalation queue Chat, and BasicQueue Voice. This counts three towards the service limit of 50.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quick connects per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>Rate of API requests</td>
<td>See Amazon Connect API throttling quotas</td>
<td>Yes</td>
<td>Account Level</td>
</tr>
</tbody>
</table>
### Amazon Connect Quotas

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
<th>Adjustability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports per instance</td>
<td>2000</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal saved reports count towards the reports per instance. For example, if one of your supervisors saves a report every day, it will count towards your overall number of saved reports per instance. As a best practice, we recommend you implement policies so reports don't pile up.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing profiles per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled reports per instance</td>
<td>50</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security profiles per instance</td>
<td>100</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task templates per instance</td>
<td>50</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task template customized fields per instance</td>
<td>50</td>
<td>No</td>
<td>Not Adjustable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Default</td>
<td>Adjustable</td>
<td>Adjustability</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Theme detection reports generated within 30 minutes per instance</td>
<td>6</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td>User hierarchy groups per instance</td>
<td>500</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This quota applies to the total number of hierarchy groups you have, across all levels. There is no feature limit for how many hierarchy groups you can have for each level. For example, one level could have 500 hierarchy groups, which would reach the quota for your instance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users per instance</td>
<td>500</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
</tbody>
</table>

**Amazon Connect AppIntegrations service quotas**

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data integration associations per data integration</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Data integrations per Region</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Event integration association</td>
<td>10</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>ons per event integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event integrations per Region</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Application per region (third-party application)</td>
<td>5</td>
<td>No</td>
</tr>
</tbody>
</table>

## Amazon Q in Connect service quotas

<table>
<thead>
<tr>
<th>Item</th>
<th>Default quotas</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistants</td>
<td>5</td>
<td>No</td>
</tr>
<tr>
<td>Knowledge bases</td>
<td>10</td>
<td>No</td>
</tr>
<tr>
<td>Assistant associations</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>Maximum size of a knowledge base</td>
<td>5GB per knowledge base</td>
<td>No</td>
</tr>
<tr>
<td>Quick responses per knowledge base</td>
<td>1,000</td>
<td>No</td>
</tr>
<tr>
<td>Content per knowledge base</td>
<td>5,000</td>
<td>No</td>
</tr>
<tr>
<td>Examples of content are frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum size per document</td>
<td>1MB</td>
<td>No</td>
</tr>
<tr>
<td>Item</td>
<td>Default quotas</td>
<td>Adjustable</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>RateLimit for all APIs</td>
<td>10TPS</td>
<td>No</td>
</tr>
<tr>
<td>The rate limit for DeleteQuickResponse and SearchQuickResponses is 20TPS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Amazon Connect Cases service quotas**

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases domains per AWS account</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Fields in a Cases domain</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>Field options per single-select field in the Cases domain</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>Layouts in a Cases domain</td>
<td>50</td>
<td>Yes</td>
</tr>
<tr>
<td>Templates in a Cases domain</td>
<td>50</td>
<td>Yes</td>
</tr>
<tr>
<td>Related items that can be attached to a case</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>Case fields per case layout</td>
<td>30</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Contact Lens service quotas

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent real-time calls with analytics</td>
<td>50</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>100 for US East (N. Virginia)</td>
<td></td>
</tr>
<tr>
<td>Concurrent post-call analytics jobs</td>
<td>200</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>See Derive Concurrent post-call analytics jobs based on your Amazon Connect call volume.</td>
<td></td>
</tr>
<tr>
<td>Concurrent post-chat analytics jobs</td>
<td>200</td>
<td>Yes</td>
</tr>
<tr>
<td>Concurrent post-contact summarization jobs</td>
<td>10</td>
<td>No</td>
</tr>
</tbody>
</table>

Derive Concurrent post-call analytics jobs based on your Amazon Connect call volume

A post-call analytics job is kicked off after the completion of each contact with Contact Lens enabled. The time to complete a post-call analytics job can vary, but for planning purposes, you can estimate that it usually takes about 40% of the call length. If you choose 40% for your estimate, to calculate concurrent post-call analytics jobs, you would use the following formula:

\[
(\text{average call duration in minutes}) \times (0.4) \times (\text{calls per hour}) / (60)
\]

The following table shows some examples of what the approximate number of concurrent post call jobs would be if you assume the time to complete the analysis is 40%.
### Average call duration (in minutes)

<table>
<thead>
<tr>
<th>Average call duration (in minutes)</th>
<th>Calls per hour*</th>
<th>Approximate Concurrent post-call jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1000</td>
<td>33</td>
</tr>
<tr>
<td>10</td>
<td>500</td>
<td>33</td>
</tr>
<tr>
<td>10</td>
<td>1000</td>
<td>67</td>
</tr>
<tr>
<td>10</td>
<td>3000</td>
<td>200</td>
</tr>
</tbody>
</table>

*For the example calculations in the preceding table, we assume a fairly uniform distribution of calls during the hour. If you have more complex traffic patterns, contact AWS Support with details about your anticipated traffic pattern.

### Amazon Connect Customer Profiles service quotas

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Connect Customer Profiles domain count</td>
<td>Each supported Region: 100</td>
<td>Yes</td>
<td>The maximum number of Amazon Connect Customer Profiles domains you can create in this account in the current AWS Region.</td>
</tr>
<tr>
<td>Keys per object type</td>
<td>Each supported Region: 10</td>
<td>Yes</td>
<td>The maximum number of keys that can be defined per object type in the current AWS Region.</td>
</tr>
<tr>
<td>Maximum expiration in days</td>
<td>Each supported Region: 1,098</td>
<td>Yes</td>
<td>The maximum expiration, in days, that can be defined for an object or profile in the current AWS Region.</td>
</tr>
<tr>
<td>Name</td>
<td>Default</td>
<td>Adjusable</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum number of calculated attributes per domain</td>
<td>Each supported Region: 50</td>
<td>No</td>
<td>The maximum number of calculated attributes per domain in the current AWS Region.</td>
</tr>
<tr>
<td>Maximum number of event stream per domain</td>
<td>Each supported Region: 1</td>
<td>No</td>
<td>The maximum number of event stream per domain in the current AWS Region.</td>
</tr>
<tr>
<td>Maximum number of integrations</td>
<td>Each supported Region: 50</td>
<td>Yes</td>
<td>The maximum number of integrations per domain in the current AWS Region.</td>
</tr>
<tr>
<td>Maximum size of all objects for a profile</td>
<td>Each supported Region: 51,200 Kilobytes</td>
<td>Yes</td>
<td>The total size of a profile, including all of its related objects, in the current AWS Region.</td>
</tr>
<tr>
<td>Object and profile maximum size</td>
<td>Each supported Region: 250 Kilobytes</td>
<td>No</td>
<td>The maximum size of a single profile or profile object in the current AWS Region.</td>
</tr>
<tr>
<td>Object types per domain</td>
<td>Each supported Region: 100</td>
<td>Yes</td>
<td>The maximum number of object types you can define per domain in the current AWS Region.</td>
</tr>
<tr>
<td>Objects per profile</td>
<td>Each supported Region: 1,000</td>
<td>Yes</td>
<td>The maximum number of objects that can be attached to a single profile in the current AWS Region.</td>
</tr>
</tbody>
</table>
Amazon Connect Outbound campaigns service quotas

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Adjustable</th>
<th>Adjustability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaigns</td>
<td>25</td>
<td>Yes</td>
<td>Resource Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This is the maximum number of campaigns that an AWS account can configure.</td>
</tr>
</tbody>
</table>

Amazon Connect Voice ID service quotas

<table>
<thead>
<tr>
<th>Item</th>
<th>Default quotas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>This quota applies per account.</td>
</tr>
<tr>
<td>Concurrent active sessions per domain</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>See the following table for information about how to derive your Concurrent active sessions quota based on your Amazon Connect call volume.</td>
</tr>
<tr>
<td>Maximum number of fraudsters per watchlist</td>
<td>500</td>
</tr>
<tr>
<td>Maximum number of watchlists per domain</td>
<td>3, including the default watchlist of a domain</td>
</tr>
<tr>
<td>Maximum number of speakers per domain</td>
<td>100,000</td>
</tr>
<tr>
<td>Active Batch Speaker Enrollment Jobs per domain</td>
<td>1</td>
</tr>
<tr>
<td>Active Batch Fraudster Registration Jobs per domain</td>
<td>1</td>
</tr>
<tr>
<td>Speakers per Batch Speaker Enrollment Job</td>
<td>10,000</td>
</tr>
</tbody>
</table>
### Default quotas

<table>
<thead>
<tr>
<th>Item</th>
<th>Default quotas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudsters per Batch Fraudster Registration Job</td>
<td>500</td>
</tr>
</tbody>
</table>

### Derive Concurrent active sessions based on your Amazon Connect call volume

Use the information in the following table to derive your quota for Voice ID Concurrent active sessions per domain. Base your quota on the number of voice calls handled by your Amazon Connect contact center where Voice ID is enabled.

<table>
<thead>
<tr>
<th>Amazon Connect Voice Contacts (Calls)/Hour*</th>
<th>Voice ID Concurrent active sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>50</td>
</tr>
<tr>
<td>5,000</td>
<td>250</td>
</tr>
<tr>
<td>10,000</td>
<td>500</td>
</tr>
<tr>
<td>20,000</td>
<td>1,000</td>
</tr>
<tr>
<td>50,000</td>
<td>2,500</td>
</tr>
</tbody>
</table>

*For the calculations in the preceding table, we assume a fairly uniform distribution of calls during the hour. If you have more complex traffic patterns, contact AWS Support with details about your anticipated traffic pattern.

### How contacts are counted

The following contacts are counted in Concurrent active calls per instance:

- Handled by a flow
- Waiting in queue
- Handled by an agent
- Outbound call
The following contacts are not counted:

- Callbacks waiting in a callback queue are not counted until the callback is offered to an available agent.
- External transfers

If the quota for **Concurrent active calls per instance** is exceeded, contacts get a reorder tone (also known as a fast busy tone), which indicates that there is no available transmission path to the called number.

You can calculate your configured quota using CloudWatch metrics. For instructions, see [Use CloudWatch metrics to calculate concurrent call quota](#).

If you're only taking calls you can also determine your **Concurrent active calls per instance** quota by doing the following:

1. Navigate to the **Edit a queue** page: choose **Routing, Queues**, and choose a queue.
2. Choose **Set a limit across all channels**.
3. Enter an exceptionally large number in the **Maximum contacts in queue** box for the contact limit.

The resulting error message displays your quota as less than the sum of the following quotas combined: **Concurrent calls per instance + Concurrent active chats per instance + Concurrent active tasks per instance**.

For example, in the following image from the **Edit queues** page, you add 1 to the error message, to get **Concurrent calls per instance + Concurrent active chats per instance + Concurrent active tasks per instance** quota = 3010.
Maximum contacts in queue

Set the maximum contacts allowed to be in the queue at the same time.

Set a limit across all channels

<table>
<thead>
<tr>
<th>Maximum contacts in queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>100000</td>
</tr>
</tbody>
</table>

You cannot have more contacts in the queue than your total queued contacts per instance quota, which is currently 3009.

The error message shows 3009 because you must set always set Maximum contacts in queue to a number that is at least 1 less than your combined quota (which is the default limit).

Amazon Connect feature specifications

Note

Feature specifications cannot be increased.

The following table lists Amazon Connect feature specifications.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent activity retention</td>
<td>24 months from the time the event occurred</td>
</tr>
<tr>
<td>File types supported for attachments to cases or chats</td>
<td>.csv, .doc, .docx, .heic, .jfif, .jpeg, .jpg, .mov, mp4, .pdf, .png, .ppt, .pptx, .rtf, .txt, .wav, .xls, .xlsx</td>
</tr>
<tr>
<td>Item</td>
<td>Feature Specification</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Maximum file size for an attachment to a case or a chat</td>
<td>20MB</td>
</tr>
<tr>
<td>Maximum timeout for an attachment scanner</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Maximum size of a real-time metrics report</td>
<td>200KB</td>
</tr>
<tr>
<td>When the Multi-Party Calls and Enhanced Monitoring feature is not enabled on your instance, the number of people who can listen in on the same agent call at the same time</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>For example, you can have a group of 5 people listen in to a call at the same time, and then a different group of 5 people listen in to a different call at the same time, and so on.</td>
</tr>
<tr>
<td></td>
<td>The total number of participants on the call would look like this:</td>
</tr>
<tr>
<td></td>
<td>1. Customer</td>
</tr>
<tr>
<td></td>
<td>2. Agent</td>
</tr>
<tr>
<td></td>
<td>3. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td></td>
<td>4. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td></td>
<td>5. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td></td>
<td>6. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td></td>
<td>7. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td>When the Multi-Party Calls and Enhanced Monitoring feature is enabled on your instance, the number of people who can be on the same agent call at the same time</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>There can be four participants in total:</td>
</tr>
<tr>
<td></td>
<td>1. Customer</td>
</tr>
<tr>
<td></td>
<td>2. Agent</td>
</tr>
<tr>
<td></td>
<td>3. Supervisor who can barge</td>
</tr>
<tr>
<td></td>
<td>4. Supervisor who can listen but not barge</td>
</tr>
<tr>
<td>Item</td>
<td>Feature Specification</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of calls that a supervisor can listen to at the same time</td>
<td>1</td>
</tr>
<tr>
<td>Quick connects you can assign to a queue</td>
<td>700</td>
</tr>
<tr>
<td>Participants on a conference call</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>The participants are the customer, agent, and others who can be agents or external third-parties.</td>
</tr>
<tr>
<td>Contact record retention</td>
<td>24 months from the time the associated contact was initiated.</td>
</tr>
<tr>
<td></td>
<td>You can choose to stream contact records to Kinesis so you can manage retention and perform advanced analysis.</td>
</tr>
<tr>
<td>Maximum size of the contact record attributes section</td>
<td>32KB</td>
</tr>
</tbody>
</table>
### Item

<table>
<thead>
<tr>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 instances can be created or deleted in 30 days</td>
</tr>
<tr>
<td>Amazon Connect enforces a limit on the total number of instances that you can create and delete in 30 days. If you exceed this limit, you will get an error message indicating there has been an excessive number of attempts at creating or deleting instances. You must wait 30 days before you can restart creating and deleting instances in your account.</td>
</tr>
<tr>
<td>For example, if you create 80 instances and delete 20 over the course of 30 days, you must wait an additional 30 days before you can create or delete any more instances. If you create and delete the same instance 100 times in 30 days, the limit also applies.</td>
</tr>
</tbody>
</table>

| Searchable custom contact attributes | 50 |
| Replica instances (created by using the ReplicatInstance API) | 5 per account |
| Traffic distribution groups | 8 per replicated instance |

### Chat feature specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachments per chat conversation</td>
<td>35</td>
</tr>
<tr>
<td>Active chats per agent</td>
<td>10</td>
</tr>
<tr>
<td>Number of custom participants on a contact</td>
<td>1</td>
</tr>
<tr>
<td>Item</td>
<td>Feature Specification</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of chat contacts that a supervisor can monitor concurrently</td>
<td>Depends on the number of concurrent chats limit set in the supervisor's routing profile</td>
</tr>
<tr>
<td>Total duration per chat</td>
<td>Up to 7 days, including wait time</td>
</tr>
<tr>
<td></td>
<td>• The default is 25 hours. You configure the chat duration using <code>StartChatContact</code> API</td>
</tr>
<tr>
<td></td>
<td>• and add the <code>ChatDurationInMinutes</code> parameter.</td>
</tr>
<tr>
<td></td>
<td>• Minimum configurable chat duration is 1 hour (60 minutes).</td>
</tr>
<tr>
<td></td>
<td>• Maximum configurable chat duration is 7 days (10,080 minutes).</td>
</tr>
<tr>
<td>Characters per chat message</td>
<td>1024</td>
</tr>
<tr>
<td>Open websocket connections per chat participant</td>
<td>5</td>
</tr>
<tr>
<td>Chat Amazon Lex bot integration timeout</td>
<td>6 seconds</td>
</tr>
<tr>
<td></td>
<td>The maximum time within which the Amazon Lex bot must respond to the chat customer's prompt.</td>
</tr>
<tr>
<td>Past chat transcript file size. This applies to <code>persistent chat</code></td>
<td>5MB</td>
</tr>
<tr>
<td>Number of past contacts that can be traversed by Amazon Connect chat</td>
<td>100</td>
</tr>
<tr>
<td>Communications widgets that can be created and customized per instance</td>
<td>15</td>
</tr>
</tbody>
</table>
# Task feature specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task templates per instance</td>
<td>50</td>
</tr>
<tr>
<td>Task template customized fields per instance</td>
<td>50</td>
</tr>
<tr>
<td>Maximum duration of a task</td>
<td>7 days</td>
</tr>
<tr>
<td>Maximum number of transfers for a task</td>
<td>11 transfers</td>
</tr>
<tr>
<td>Maximum number of linked tasks on an existing contact</td>
<td>11</td>
</tr>
</tbody>
</table>

# Forecasting, capacity planning, and scheduling feature specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents per schedule generation run</td>
<td>800</td>
</tr>
<tr>
<td>Agents per staffing group</td>
<td>80</td>
</tr>
<tr>
<td>Capacity plans per instance</td>
<td>500</td>
</tr>
<tr>
<td>Capacity scenarios per instance</td>
<td>500</td>
</tr>
<tr>
<td>Capacity plan user data uploads per instance</td>
<td>500</td>
</tr>
<tr>
<td>Capacity plan override uploads per instance</td>
<td>5000</td>
</tr>
<tr>
<td>Concurrent uploads per instance</td>
<td>20</td>
</tr>
<tr>
<td>File size per upload of agent time off data</td>
<td>1GB</td>
</tr>
<tr>
<td>File size per upload of time off group allowance data</td>
<td>1GB</td>
</tr>
<tr>
<td>The .csv file can cover up to 13 months.</td>
<td></td>
</tr>
<tr>
<td>File size per upload of capacity plan user data</td>
<td>1GB</td>
</tr>
</tbody>
</table>
### Item | Feature Specification
--- | ---
File size per upload of capacity plan overrides | 250MB
File size per upload of forecast overrides | 250MB
File size per upload of historical actuals | 1GB
Forecast groups per instance | 500
Forecast override uploads per instance | 500
Historical actuals uploads per instance | 50
Queues per forecast group | 200
Schedules per instance | 600
Shift activities per instance | 300
Shift activities per shift profile | 10
Shift profiles per instance | 1300
Staffing groups per forecast group | 100
Staffing groups per instance | 1300
Staffing groups per supervisor/manager | 45
Supervisors/managers per staffing group | 40

**Integration association resource feature specifications**

The following table lists feature specifications for the integration association resource. It lists how many of each type of integration association resource can be ingested.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment scanner</td>
<td>1</td>
</tr>
</tbody>
</table>
### Item | Feature Specification
--- | ---
Voice ID domain | 1
Amazon Pinpoint app | 1
Event | 10
The event integration resource is used for task triggers.
Amazon Q in Connect assistant | 1
Amazon Q in Connect knowledge base | 10
Cases domain | 1

**Amazon Connect Contact Lens feature specifications**

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom vocabularies</td>
<td>20</td>
</tr>
<tr>
<td>Contact Lens rules for post-call</td>
<td>500</td>
</tr>
<tr>
<td>Contact Lens rules for post-chat</td>
<td>500</td>
</tr>
<tr>
<td>Contact Lens rules for real-time</td>
<td>500</td>
</tr>
</tbody>
</table>

**Evaluation forms feature specifications**

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of evaluation forms per instance</td>
<td>50</td>
</tr>
</tbody>
</table>

Historical versions are not counted, only form names are counted.
### Feature Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of versions per form</td>
<td>50</td>
</tr>
<tr>
<td>Maximum number of sections per form</td>
<td>100</td>
</tr>
<tr>
<td>Maximum number of questions per form</td>
<td>100</td>
</tr>
<tr>
<td>Maximum nesting level of sections</td>
<td>2 (sections can have sub-sections, but sub-sections cannot have sub-sub-sections)</td>
</tr>
<tr>
<td>Definition title length</td>
<td>1-128 characters</td>
</tr>
<tr>
<td>Section title length</td>
<td>1-128 characters</td>
</tr>
<tr>
<td>Question title length</td>
<td>1-350 characters</td>
</tr>
<tr>
<td>Section instructions length</td>
<td>up to 1024 characters</td>
</tr>
<tr>
<td>Number of answer options for single select questions</td>
<td>2-256 answer options</td>
</tr>
<tr>
<td>Answer option text length for single select questions</td>
<td>1-128 characters</td>
</tr>
</tbody>
</table>

### Amazon Connect Rules feature specifications

The following table lists feature specifications for Amazon Connect Rules.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions in a rule</td>
<td>20</td>
</tr>
<tr>
<td>Rules per event source type</td>
<td>500</td>
</tr>
<tr>
<td>Condition type</td>
<td>Number of entries or selections</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Evaluation - Form score</td>
<td>20</td>
</tr>
<tr>
<td>Evaluation - Section score</td>
<td>20</td>
</tr>
<tr>
<td>Evaluation - Question score</td>
<td>20</td>
</tr>
<tr>
<td>Evaluation - Results available</td>
<td>20</td>
</tr>
<tr>
<td>Words or phrases - Exact match</td>
<td>100</td>
</tr>
<tr>
<td>Words or phrases - Semantic match</td>
<td>4</td>
</tr>
<tr>
<td>Words or phrases - Pattern match</td>
<td>100</td>
</tr>
<tr>
<td>Queue condition</td>
<td>100</td>
</tr>
<tr>
<td>Agent condition</td>
<td>100</td>
</tr>
<tr>
<td>Custom attributes</td>
<td>5</td>
</tr>
<tr>
<td>Sentiment - Time period</td>
<td>5</td>
</tr>
<tr>
<td>Condition type</td>
<td>Number of entries or selections</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Sentiment - Entire contact</td>
<td>5</td>
</tr>
<tr>
<td>Interruptions</td>
<td>5</td>
</tr>
<tr>
<td>Response time</td>
<td>4 hours</td>
</tr>
<tr>
<td>Non-talk time</td>
<td>5 hours</td>
</tr>
</tbody>
</table>

**Countries you can call by default**

The Region where your instance is created determines which countries you can call by default.

For a list of all the countries available for outbound calling, see Amazon Connect pricing.

If you already have an instance, the countries that you are allowed to call may be different that those listed in the following sections because we have changed the service quotas over time.

**Prefixes that are not allowed by default**

**UK** mobile numbers with the following prefix are not allowed by default:

- +447

Before you can dial these UK mobile numbers, you must submit a service quota increase request.

**Japan** mobile numbers with the following prefixes are not allowed by default:

- +8170, 8180, and 8190

Before you can dial these Japan mobile numbers, you must submit a service quota increase request.

**How to allow calling to additional countries**

Use the following instructions to allow calling to additional countries, or to limit the countries that you can call from.
Note

Starting Friday, December 01, 2023, Amazon Connect Country Allow-listing for Outbound Calls requests will move to the Account and billing section of the AWS Support Center console. To create a new support case for Country Allow-listing for Outbound Calls, you will choose Account and billing, and then choose Amazon Connect (Number Management) from the Services dropdown menu.

1. Choose Account and billing to go to the pre-populated form in the AWS Support console. You must be signed in to your AWS account to access the form.

2. For Service, Connect (Number Management) should be selected.

3. For Category, Country Allow-listing for Outbound Calls should be selected.

4. Select the required severity.

5. Choose Next step: Additional information

6. On the Additional information page:
   a. Enter the subject.
   b. Under Description, list which countries you want to allow calling to, or limit calling from.

7. Choose Next step: Solve now or contact us.

8. On the Solve now or contact us page:
   - Choose the Contact us tab and select your Preferred contact language and your preferred contact method.

9. Choose Submit.

10. The Amazon Connect team will review your ticket and get back to you.

**Instances created in US East, US West, Canada (Central) and AWS GovCloud (US-West)**

You can call the following countries by default:

- United States
- Canada
- Mexico
- Puerto Rico
- United Kingdom: See [Prefixes that are not allowed by default](#)

**Instances created in Africa (Cape Town)**

You can call the following countries by default:

- South Africa
- United Kingdom
- United States

**Instances created in Asia Pacific (Seoul)**

You can call the following countries by default:

- South Korea
- United Kingdom
- United States

**Instances created in Asia Pacific (Singapore)**

You can call the following countries by default:

- Singapore
- Australia
- Hong Kong
- United States
- United Kingdom: See [Prefixes that are not allowed by default](#)

**Instances created in Asia Pacific (Sydney)**

You can call the following countries by default:

- Australia
• New Zealand
• United States

**Instances created in Asia Pacific (Tokyo)**

You can call the following countries by default:

• Japan: See [Prefixes that are not allowed by default](#)
• Vietnam
• United States

**Instances created in EU (Frankfurt) and EU (London)**

You can call the following countries by default:

• United Kingdom: See [Prefixes that are not allowed by default](#)
• Italy
• France
• Ireland
• United States

**API throttling quotas**

**Amazon Connect API throttling quotas**

Amazon Connect throttling quotas are by account, and per Region, not by user and not by instance. For example:

• If different users from the same account make requests, they are sharing a throttle bucket.
• If multiple requests are sent from different instances from the same account, they are also sharing a throttle bucket.

When you use the [Amazon Connect Service API](#), the number of requests per second is limited to the following:
• For the `GetMetricData` and `GetCurrentMetricData` operations, a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second. For `GetMetricData`, you cannot increase throttle limits.

  The default limits for `GetMetricDataV2` are 10 requests per second.

• For `StartChatContact`, `StartContactStreaming`, `StopContactStreaming`, `CreateParticipant` a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second.

• For all `Evaluations actions`, the throttling quota is 1 request per second.

• For all other operations, a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.

### Amazon Connect Participant Service API throttling quotas

For the Amazon Connect Participant Service, the quotas are by instance.

When you use the Amazon Connect Participant Service API, the number of requests per second is limited to the following:

• `CompleteAttachmentUpload`: a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.

• `CreateParticipantConnection`: a RateLimit of 6 requests per second, and a BurstLimit of 9 requests per second.

• `DisconnectParticipant`: a RateLimit of 3 requests per second, and a BurstLimit of 5 requests per second.

• `GetAttachment`: a RateLimit of 8 requests per second, and a BurstLimit of 12 requests per second.

• `GetTranscript`: a RateLimit of 8 requests per second, and a BurstLimit of 12 requests per second.

• `SendMessage` and `SendEvent`: a RateLimit of 10 requests per second, and a BurstLimit of 15 requests per second.

• `StartAttachmentUpload`: a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.

### Amazon Connect Contact Lens Service API throttling quotas

Amazon Connect Contact Lens throttling quotas are by account, not by user and not by instance. For example:
• If different users from the same account make requests, they are sharing a throttle bucket.

• If multiple requests are sent from different instances from the same account, they are also sharing a throttle bucket.

When you use the Amazon Connect Contact Lens API, the number of requests per second is limited to the following:

• ListRealtimeContactAnalysisSegments: a RateLimit of 1 request per second, and a BurstLimit of 2 requests per second.

Amazon Connect Cases API throttling quotas

<table>
<thead>
<tr>
<th>API</th>
<th>Default TPS throttling limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateCase, SearchCases, UpdateCase, AssociateContact, ListTemplates, CreateRelatedItem, SearchRelatedItems</td>
<td>10</td>
</tr>
<tr>
<td>CreateField, ListFields, CreateDomain, GetDomain, CreateTemplate, BatchPutFieldOptions, CreateLayout, UpdateLayout, UpdateTemplate, UpdateField</td>
<td>5</td>
</tr>
<tr>
<td>BatchGetField</td>
<td>25</td>
</tr>
<tr>
<td>GetCase</td>
<td>15</td>
</tr>
<tr>
<td>GetTemplate, GetLayout</td>
<td>20</td>
</tr>
<tr>
<td>ListFieldOptions</td>
<td>15</td>
</tr>
</tbody>
</table>

Customer Profiles API throttling quotas

<table>
<thead>
<tr>
<th>API</th>
<th>Default TPS throttling limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListDomains</td>
<td>5</td>
</tr>
<tr>
<td>API</td>
<td>Default TPS throttling limits</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>GetDomain</td>
<td>5</td>
</tr>
<tr>
<td>CreateDomain</td>
<td>1</td>
</tr>
<tr>
<td>UpdateDomain</td>
<td>1</td>
</tr>
<tr>
<td>DeleteDomain</td>
<td>1</td>
</tr>
<tr>
<td>ListProfileObjectTypes</td>
<td>5</td>
</tr>
<tr>
<td>GetProfileObjectType</td>
<td>10</td>
</tr>
<tr>
<td>PutProfileObjectType</td>
<td>1</td>
</tr>
<tr>
<td>DeleteProfileObjectType</td>
<td>1</td>
</tr>
<tr>
<td>ListProfileObjectTypeTemplates</td>
<td>5</td>
</tr>
<tr>
<td>GetProfileObjectTypeTemplate</td>
<td>5</td>
</tr>
<tr>
<td>ListIntegrations</td>
<td>5</td>
</tr>
<tr>
<td>GetIntegration</td>
<td>5</td>
</tr>
<tr>
<td>PutIntegration</td>
<td>1</td>
</tr>
<tr>
<td>DeleteIntegration</td>
<td>1</td>
</tr>
<tr>
<td>ListIdentityResolutionJobs</td>
<td>5</td>
</tr>
<tr>
<td>GetIdentityResolutionJob</td>
<td>5</td>
</tr>
<tr>
<td>GetAutoMergingPreview</td>
<td>1</td>
</tr>
<tr>
<td>CreateEventStream</td>
<td>1</td>
</tr>
<tr>
<td>ListEventStreams</td>
<td>5</td>
</tr>
<tr>
<td>DeleteEventStream</td>
<td>5</td>
</tr>
<tr>
<td>API</td>
<td>Default TPS throttling limits</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>GetEventStream</td>
<td>5</td>
</tr>
<tr>
<td>CreateCalculatedAttributeDefinition</td>
<td>1</td>
</tr>
<tr>
<td>GetCalculatedAttributeDefinition</td>
<td>5</td>
</tr>
<tr>
<td>UpdateCalculatedAttributeDefinition</td>
<td>1</td>
</tr>
<tr>
<td>DeleteCalculatedAttributeDefinition</td>
<td>5</td>
</tr>
<tr>
<td>ListCalculatedAttributeDefinitions</td>
<td>5</td>
</tr>
<tr>
<td>CreateIntegrationWorkflow</td>
<td>5</td>
</tr>
<tr>
<td>DeleteWorkflow</td>
<td>5</td>
</tr>
<tr>
<td>ListWorkflows</td>
<td>5</td>
</tr>
<tr>
<td>GetWorkflow</td>
<td>5</td>
</tr>
<tr>
<td>GetWorkflowSteps</td>
<td>5</td>
</tr>
<tr>
<td>SearchProfiles</td>
<td>100</td>
</tr>
<tr>
<td>ListProfileObjects</td>
<td>100</td>
</tr>
<tr>
<td>GetMatches</td>
<td>100</td>
</tr>
<tr>
<td>GetSimilarProfiles</td>
<td>100</td>
</tr>
<tr>
<td>ListRuleBasedMatches</td>
<td>5</td>
</tr>
<tr>
<td>GetCalculatedAttributeForProfile</td>
<td>100</td>
</tr>
<tr>
<td>ListCalculatedAttributesForProfile</td>
<td>100</td>
</tr>
<tr>
<td>CreateProfile</td>
<td>100</td>
</tr>
<tr>
<td>UpdateProfile</td>
<td>100</td>
</tr>
<tr>
<td>API</td>
<td>Default TPS throttling limits</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>PutProfileObject</td>
<td>100</td>
</tr>
<tr>
<td>AddProfileKey</td>
<td>100</td>
</tr>
<tr>
<td>DeleteProfile</td>
<td>100</td>
</tr>
<tr>
<td>DeleteProfileObject</td>
<td>100</td>
</tr>
<tr>
<td>DeleteProfileKey</td>
<td>100</td>
</tr>
<tr>
<td>MergeProfiles</td>
<td>100</td>
</tr>
<tr>
<td>TagResource</td>
<td>5</td>
</tr>
<tr>
<td>UntagResource</td>
<td>5</td>
</tr>
<tr>
<td>ListTagsForResource</td>
<td>5</td>
</tr>
<tr>
<td>ListAccountIntegrations</td>
<td>100</td>
</tr>
</tbody>
</table>

**Amazon Connect Voice ID Service API throttling quotas**

<table>
<thead>
<tr>
<th>API</th>
<th>Default TPS throttling limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvaluateSession</td>
<td>60</td>
</tr>
<tr>
<td>Domain APIs: CreateDomain, DescribeDomain, UpdateDomain, DeleteDomain, ListDomains</td>
<td>2</td>
</tr>
<tr>
<td>Batch APIs: StartSpeakerEnrollmentJob, DescribeSpeakerEnrollmentJob, ListSpeakerEnrollmentJobs, StartFraudsterRegistrationJob, DescribeFraudsterRegistrationJob, ListFraudsterRegistrationJobs</td>
<td>5</td>
</tr>
<tr>
<td>ListSpeakers</td>
<td>5</td>
</tr>
<tr>
<td>API</td>
<td>Default TPS throttling limits</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>DescribeSpeaker, OptOutSpeaker, DeleteSpeaker, DescribeFraudster, DeleteFraudster</td>
<td>10</td>
</tr>
<tr>
<td>CreateIntegrationAssociation, DeleteIntegrationAssociation, ListIntegrationAssociation</td>
<td>2</td>
</tr>
<tr>
<td>TagResource, UnTagResource, ListTagsForResource</td>
<td>2</td>
</tr>
</tbody>
</table>
Get started with Amazon Connect

Use these steps to set up your contact center.

1. **Create an Amazon Connect instance.** Use an instance to contain all the resources and settings related to your contact center. You specify how you plan to manage user accounts, whether your contact center will accept incoming calls and make outbound calls, and review the location where data will be stored in your Amazon S3 bucket.

2. **Set up phone numbers to use the Amazon Connect service.** If you're using voice, either claim a phone number that AWS provides, or port your current phone number to Amazon Connect. If you choose to port your numbers, we suggest claiming a number so you can test Amazon Connect and build your contact center while waiting for your numbers to be ported over.

3. **Set up routing.** Create your queues and routing profiles, and set your hours of operation. In your routing profiles, specify the channels that agents should use: voice, chat, tasks, or all three. You also specify how many chats and tasks an agent can manage at the same time.

4. **Create Amazon Connect Flows.** Establish a flow to define the customer experience with your contact center from start to finish. A single flow works for voice, chat, and tasks, which makes your design more efficient. When you build flows and configure the blocks, indicate how the flow should work for voice, chat, and tasks.

5. Add users, which are your managers and agents, and configure their settings. Assign a routing profile to each agent, specify whether they are using a softphone or desk phone, and set how long they have for **After contact work.** For instructions, see [Add users to Amazon Connect](#) and [Set up agents](#).

6. If you're using chat, we provide several tools to help you enable your customer-facing app to engage with Amazon Connect chat. For more information, see [Set up your customer's chat experience](#).

**Next steps**

There's a lot you can do to optimize your contact center. Here are a couple of additional steps that you may find useful:

1. **Set up recording behavior.** Monitor live conversations and review past conversations. This is a way that managers can coach agents and help them improve. For voice conversations, set up recording in your flows. For chat conversations, set up recording at the instance level.
To learn how to monitor conversations, see [Set up live monitoring for voice and/or chat](https://aws.amazon.com/connect/monitoring/).

2. **Add an Amazon Lex bot to Amazon Connect.** Use Amazon Lex in your contact center to reduce the load on your agents. For example, a bot can handle the initial interaction before the chat is routed to an agent, and also answer common questions for the customer.

### Take a free online class

Check out the following free online classes:

- [Introduction to Amazon Connect and the Contact Control Panel (CCP)](https://aws.amazon.com/connect/learn/)
- [Amazon Connect: Introduction to the Administrative Interface](https://aws.amazon.com/connect/learn/)
- [Amazon Connect: Creating and Managing Amazon Connect Instances](https://aws.amazon.com/connect/learn/)
- [Amazon Connect: Implementing Chat in Amazon Connect](https://aws.amazon.com/connect/learn/)
- [Amazon Connect: Implementing Tasks in Amazon Connect](https://aws.amazon.com/connect/learn/)

### Amazon Connect concepts

Amazon Connect enables you to create an **omnichannel contact center**: a contact center that provides a unified experience across multiple channels, such as voice, chat and SMS messaging, and tasks.

- You use the same routing profiles, queues, flows, metrics, and reports for all channels.
- Managers monitor all channels from one dashboard.
- Agents handle all customers from just one interface. If a customer interaction starts with chat and moves to voice, the agent handling the voice call has the complete chat transcript so context is preserved.

You can create highly personalized experiences for your customers using omnichannel communications, and separate the channels where needed. For example, you can dynamically offer chat and/or voice contact based on such factors as customer preference, estimated wait times, and agent skill.

This section explains concepts that will help you set up your Amazon Connect contact center, whether you use one channel or more.
Amazon Connect provides a variety of choices to enable your company to make and receive telephone calls. One of the great advantages of Amazon Connect is AWS manages the telephony infrastructure for you: carrier connections, redundancy, and routing. And, it's designed to scale.

This topic explains the options that Amazon Connect provides for telephony, which helps you build a solution to meet your business requirements.

**Contents**

- Telephony architecture
- Use cases for different configurations

**Telephony architecture**

Amazon Connect provides capabilities to host both toll-free and direct dial numbers (DID) in all AWS Regions supported by Amazon Connect. You can use both types of numbers in a single...
instance. A complete list of supported countries/regions and costs is located on the Amazon Connect pricing page.

AWS manages the connectivity to our network of carriers providing diverse connections to multiple carriers in each region supported by Amazon Connect. When Amazon Connect is deployed in a Region, we take advantage of the built-in redundancy of the AWS Availability Zone design to provide multiple carrier interfaces into multiple data centers. You can see how AWS manages the design of a Region here.

In addition to the Amazon Connect service being spread across multiple Availability Zones, AWS also has multiple telephony providers. These providers have multiple links into the data centers in those Availability Zones. This ensures that if a single or even multiple links fail from a carrier, there are alternate routes available to ensure the service remains available.

To learn more about Amazon Connect architecture, see Architectural guidance for Amazon Connect.

- **AWS manages toll-free numbers as a Responsible Organization**

  These numbers are phone numbers with distinct prefix codes that can be dialed with no charge to the person placing the call. Such numbers allow callers to reach businesses and/or individuals out of the area without being charged a long-distance fee for the call.

  In the United States, the Federal Communications Commission provides rules for obtaining and using toll-free numbers. In other countries, similar governing bodies ensure that such numbers are managed and distributed in accordance with local laws.

  When you claim or port a US toll-free number into Amazon Connect, we register that number with SOMOS. After the number is registered, we are able to select multiple carriers to provide BOTH route and carrier redundancy. This provides the highest level of availability, ensuring the number will remain available even in the event of a complete carrier outage. This level of service does come at an additional cost, as these numbers are a higher price than direct dial, but the service reliability and customer experience make this the most attractive option.

- **Locally formatted numbers**

  Direct inward dialing (DID), also called direct dial-in (DDI) in Europe, is a telecommunication service offered by telephone companies to subscribers. DID numbers provide a locally formatted telephone number that can match the dialing pattern of a local subscriber. For example, in
Seattle, Washington, USA, the local dialing pattern is +1(206)-NXX-XXXX. The provider of the DID number would provide numbers with the +1(206) pattern to match local dialing.

In the United States, DID numbers are regulated by State Public Utilities commissions. DID numbers are managed by a single carrier. While they are portable, they can't be load balanced/managed across multiple carriers. This makes them less reliable than toll-free numbers.

DID numbers offer you the ability to present a local calling line identification when placing outbound calls, and a local presence to inbound callers. This can be very useful to increase the likelihood outbound and queued callback calls get answered by your customers. It can also show a customer that you are local to their area, and provide a cheaper inbound route than a long-distance call if you don't publish a toll-free number.

Because DID numbers are threaded to single carrier, Amazon Connect doesn't offer carrier redundancy for DID numbers. We do offer link redundancy across multiple Availability Zones, so in the event of a link failure that carrier still has facilities available in another location to deliver calls. DID numbers also have a capacity limitation on how many calls a single number can accommodate, and this number does vary by Region. It is important to work with your AWS account team to ensure you are properly enabled with the right type of DID numbers if you plan on using DID numbers as your primary inbound channel, and have an expectation of over 100 concurrent calls per number.

DID numbers are less expensive than toll-free numbers, but don't have the redundancy and broad geographical coverage of them. The ability to localize numbers may be an attractive option for your business.

Use cases for different configurations

Starting fresh with Amazon Connect

In this case, simply select new numbers using the claim a number process. For instructions, see How to get an Amazon Connect phone number in your current country.

Migrating to Amazon Connect from another provider/platform

If you're migrating to Amazon Connect from other platform, we recommend starting with a proof of concept, and migrating to Amazon Connect over time.

- A best practice is to forward your existing numbers to a new number (or numbers) claimed in Amazon Connect until you are fully converted.
• After fully converting, use the porting process to bring your numbers into Amazon Connect.
• This gives you a fallback in case you have migration issues.

Maintaining two separate platforms

In some cases, you may have more than one Contact Center platform requiring telephony. Here's an overview of how to configure this:

• Choose which platform is the initial call-handling service, and forward to the other platform.
• If Amazon Connect is the primary call handling platform, you can port or claim numbers. You will design your flows to transfer calls to the other platform on a telephone number you will provide in the flow.
• If the external platform is the primary call handler, you will need to configure that platform to forward calls to a number you claim in Amazon Connect. Choose either a toll-free number, which will give you better redundancy and capacity at an increased cost, or a bank of DID numbers to terminate the call into Amazon Connect.
• For the use case, we recommend that you engage AWS Solution Architecture support to ensure your contact center is well-architected to achieve the best possible outcomes.

Concepts: Web and mobile messaging capabilities in Amazon Connect

⚠️ Important
If you found this page because you need to contact Amazon for support, see Amazon Customer Service (Amazon orders and deliveries) or AWS Support (Amazon Web Services).

Amazon Connect lets you build chat messaging features—mobile chat, web chat, SMS, and third-party messaging services—into your website and mobile apps. It enables your customers to start chatting with contact center agents from any of your business applications, web or mobile.

Interactions are asynchronous, enabling your customers to start a chat with an agent or Amazon Lex bot, step away from it, and then resume the conversation again. They can even switch devices and continue the chat.

Contents
• Multiple channels, one experience
Multiple channels, one experience

Agents have a single user interface to help customers using voice, chat, and tasks. This reduces the number of tools that agents have to learn and the number of screens they have to interact with.

Chat activities integrate into your existing contact center flows and the automation that you built for voice. You build your flows once and reuse them across multiple channels.

Metrics collection and the dashboards you built automatically benefit from the unified metrics across multiple channels.

Getting started

To add chat messaging capabilities to your Amazon Connect contact center and allow your agents to engage in chats, perform the following steps:

- Chat is enabled at the instance level when an Amazon S3 bucket is created for storing chat transcripts.
- Add chat to your agent's routing profile.
- Optionally, you can set up chat subtypes such as SMS messaging. You procure an SMS-enabled phone number by using Amazon Pinpoint SMS, import it into Amazon Connect, and then assign it to your flows. For more information, see:
  - Request an SMS-enabled phone number through Amazon Pinpoint SMS
  - Set up SMS messaging

Agents can then begin accepting chats through the Contact Control Panel.

You can see real-time and historical metrics for the chat messaging channel (for example, arrival time, handle time) as part of their overall Chat channel metrics in the same reporting experience used for calls/chats/tasks in order to assess agent performance and productivity.
Amazon Connect provides several resources to help you add chat to your website. For more information, see Set up your customer's chat experience.

**Example chat scenario**

A customer and agent are chatting. The customer stops responding to the agent. The agent asks "Are you there?" and doesn't get a reply. The agent leaves the chat. Now the chat is no longer associated with an agent. Your flow determines what happens next.

In this scenario, the customer eventually sends another message ("Hey, I'm back") and the chat resumes. Depending on the logic that you define in the flow, the chat can be assigned to the original agent, or a different agent or queue.

Here's how you build this scenario:

1. Create a disconnect flow. The following image shows the Sample disconnect flow in the flow designer. This flow includes the following connected blocks: Play prompt, Wait which branches to three Play prompts (for Customer returned, Time expired, and Error), then Transfer to queue and Disconnect.

2. In the disconnect flow, add a Wait block. The Wait block has two branches:
• **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. The total duration of the chat, including multiple **Wait** blocks, cannot exceed 25 hours.

For example, for this branch you might just want to run a **Disconnect** block and end the chat.

• **Customer return**: Run this branch when the customer returns and sends a message. With this branch, you can route the customer to the previous agent, previous queue, or set a new working queue or agent.

3. In your inbound flow, add the **Set Disconnect Flow** block. Use it to specify that when the agent or Amazon Lex bot has disconnected from the chat and only the customer remains, the set disconnect flow should run.

In the following block, for example, we specified that the **Sample disconnect flow** should run.

For an example that uses the **Set disconnect flow** block, see the **Sample inbound flow**.

**When do chats end?**

By default, the duration for a chat conversation, including the time spent waiting when the customer isn't active, can't exceed 25 hours. However, you can change this default duration and instead configure a custom chat duration. You can configure a chat to last from a minimum of 1 hour (60 minutes) to up to 7 days (10,080 minutes). To configure a custom chat duration, call the **StartChatContact** API and add the **ChatDurationInMinutes** parameter.
During an ongoing chat session, there's no limit to the number of times a customer can leave and rejoin an existing ongoing chat session. To accomplish this, use the **Wait** block. For example, you might wait 12 hours for the customer to resume the chat before ending the chat session. If the customer tries to resume the chat after 12 hours, in the flow you can have an Amazon Lex bot ask if they're contacting you about the same issue or a different one.

By specifying a wait time that's significantly shorter than the chat duration, you help ensure that customers have a good experience. For instance, for a 25-hour duration chat, it's possible for the customer to resume a chat after 24 hours and 58 minutes, and then be cut off after two minutes because the conversation ends at the 25-hour limit.

![Tip]

If you're using Amazon Lex with chat, note that the default session timeout for an Amazon Lex session is 5 minutes. The total duration for a session can't exceed 24 hours. To change the session timeout, see [Setting the Session Timeout](https://docs.aws.amazon.com/AmazonConnect/latest/AdminGuide/) in the *Amazon Lex Developer Guide*.

**Pricing**

Chat is charged on a per use basis. There are no required up-front payments, long-term commitments, or minimum monthly fees. You pay per chat message, independently of the number of agents or customers using it. Regional pricing may vary. For more information, see Amazon Connect pricing.

**More information**

For more information about chat, see the following topics:

- Test voice, chat, and task experiences
- How routing works with multiple channels
- Create a routing profile
- Amazon Connect Chat SDK and Sample Implementations
Concepts: Tasks in Amazon Connect

⚠ Important
If you found this page because you need to contact Amazon for support, see Amazon Customer Service (Amazon orders and deliveries) or AWS Support (Amazon Web Services) instead.

Amazon Connect Tasks allows you to prioritize, assign, track, and even automate tasks across the disparate tools agents use to support customers. For example, using Tasks you can:

- Follow-up on customer issues recorded in a customer relationship management (CRM) solution such as Salesforce.
- Follow-up with a customer through a call.
- Complete actions in a business-specific system, such as processing a customer claim in an insurance application.

Currently, Amazon Connect Tasks can be used in compliance with GDPR and is approved for SOC, PCI, HITRUST, ISO, and HIPAA.

What is a task?

In a business a task is a unit of work that an agent must complete. This includes work that may have originated in external applications. In Amazon Connect this unit of work is a contact. It's routed, prioritized, assigned, and tracked just like a voice or chat contact. Everything that is applicable to a voice or chat contact is also applicable to a task contact.

Agents handle tasks in their Contact Control Panel (CCP), again just like any other contact. When assigned a task, agents see a notification with the description of the task, information associated with the tasks, and links to any applications that they might need to complete the task. The following image shows what an agent's CCP may look like when they manage tasks.
How to create tasks

Amazon Connect provides different ways for you to create tasks:

1. You can use pre-built connectors with CRM applications (for example, Salesforce and Zendesk) to automatically create tasks based on a set of pre-defined conditions, without any custom development.

   For example, you can configure a rule in Amazon Connect to automatically create a task when a new case is created in Salesforce.

   For more information, see Set up applications for task creation and Create rules that generate tasks for third-party integrations.

2. You can integrate with your homegrown or business-specific applications to create tasks using Amazon Connect APIs.
For more information, see the StartTaskContact API.

3. You can add a Create task block to your flows. This block enables you to create and orchestrate tasks directly from flows based on customer input (DTMF input), and contact and tasks information.

4. You can enable your agents to create tasks from the Contact Control Panel (CCP) without you doing any development work.

   For example, agents can create tasks to ensure follow up work is not forgotten, such as calling a customer back to provide a status update on their issue.

   For more information, see Test voice, chat, and task experiences.

For more information on getting started with tasks, see Set up tasks.

**Supported flow types**

You can use tasks in the following flow types:

- Inbound flow
- Customer queue flow
- Agent whisper flow
- Transfer to queue flow
- Transfer to agent flow

**Supported contact blocks**

You can use tasks in the following flow blocks:

- Change routing priority/age
- Check contact attributes
- Check hours of operation
- Check queue status
- Check staffing
- Create task
- Disconnect / hang up
- Distribute by percentage
- End flow / resume
- Get queue metrics
- Invoke AWS Lambda function
- Loop
- Set contact attributes
- Set customer queue flow
- Set disconnect flow
- Set working queue
- Transfer to flow
- Transfer to queue
- Wait

**Linked tasks**

When using tasks with the [StartTaskContact](https://docs.aws.amazon.com/forecast/latest/APIReference/API_StartTaskContact.html) API, a new contact can be associated with an existing contact through `PreviousContactID` or `RelatedContactId`. This new contact contains a copy of the contact attributes from the linked contact.

The following code shows request syntax that includes `PreviousContactID` and `RelatedContactId`.

```
PUT /contact/task HTTP/1.1
Content-type: application/json

{
    "Attributes": {
        "string" : "string"
    },
    "ClientToken": "string",
    "ContactFlowId": "string",
    "Description": "string",
    "InstanceId": "string",
    "Name": "string",
    "PreviousContactId": "string",
    "QuickConnectId": "string",
```
When you use PreviousContactID or RelatedContactID to create tasks, note the following:

- **PreviousContactID** - When contacts are linked using the PreviousContactID, updates that are made to contact attributes at any time in the chain will percolate through the entire chain. There can be a maximum of 12 linked contacts in a chain.

- **RelatedContactID** - When contacts are linked using the RelatedContactID, updates that are made to contact attributes will percolate only to the contactID that is referenced in the UpdateContactAttributes API.

The limit of 12 contacts in a chain does not apply when you use RelatedContactID to create a task.

**Note**

You can specify only PreviousContactID or RelatedContactID in a request body, but not both. If you do specify both, Amazon Connect returns an InvalidRequestException error with a 400 status code.

For information about how PreviousContactID and RelatedContactId are modeled in contact records, see [ContactTraceRecord](#) in the contact records data model.

**Using IAM? Add Task permissions**

If your organization is using custom [IAM](#) policies to manage access to the Amazon Connect console, make sure users have the appropriate permissions to set up applications for task creation. For a list of required permissions, see [Tasks page](#).
Note

If your instance was created before October 2018, for information about how to configure your service-linked roles (SLR), see For instances created before October 2018.

Track tasks in real-time and historical metrics reports

You can track the status of all tasks in real-time and historical metrics reports, just like you track contacts in other channels. For example, you can track:

- How long agents spent working on each task (Agent on contact time).
- The total time from when a task was created to when it was completed. (Contact handle time).

There are a few metrics that don't apply to tasks so you'll notice a value of 0 on the report for them:

Real-time metrics

- Avg interaction and hold time
- Avg hold time

Historical metrics

- Agent interaction and hold time
- Agent interaction time
- Average agent interaction time
- Average customer hold time

Manage tasks to custom service levels (SL)

While voice and chats may have short service level times based on seconds or minutes, you may have some tasks with service levels that are hours or days. You can create custom service level durations that are appropriate to each of your channels. For more information, see real-time custom service levels and historical custom service levels.
When do tasks end?

The total duration of a task can be up to 7 days. A task ends when one of the following happens:

- An agent completes the task.
- A flow runs a Disconnect / hang up block, which ends the task.
- A task reaches the 7 day limit.
- You end the task using the StopContact API.

Search and review completed tasks

Use the Contact search page to search for and review completed tasks.

The following image is an example of what the Contact Summary and References look like in a contact record for a task.
The following data is appended to the contact record but not stored with it. The data is included in an export.

- Flow ID
- Potential attributes:
  - **ContactDetails**
    - Name: the name of the task
    - Description: the description of the task
  - **References**: any links to forms or other sites

When task is scheduled for a future date and time, **Contact Summary** also displays **Scheduled time**.

**More information**

- [Amazon Connect feature specifications](#)
- [Accept a task](#)
- [Create a new task](#)
- [Transfer a task](#)

**Concepts: Routing profiles**

A routing profile determines what types of contacts an agent can receive and the routing priority.

- Each agent is assigned to one routing profile.
- A routing profile can have multiple agents assigned to it.
Amazon Connect uses routing profiles to allow you to manage your contact center at scale. To quickly change what a group of agents does, you only need to make an update in one place: the routing profile.

**Default routing profile: Basic routing profile**

Amazon Connect includes a default routing profile named **Basic routing profile**. Along with the [default flows](#) and default queue (named **BasicQueue**), it powers your contact center so you don't need to do any customization. This is what enables you to get started quickly.

**Routing Profiles Link Queues and Agents**

When you create a routing profile, you specify:

- The channels the agents will support.
- The queues of customers that the agents will handle. You can use a single queue to handle all incoming contacts, or you can set up multiple queues. Queues are linked to agents through a routing profile.
- Priority and delay of the queues.

The following image shows a graphic of a group of agents mapped to a routing profile. The routing profile specifies multiple channels and queues for the agents.
Concepts: Standard queues and agent queues

There are two types of queues:

- **Standard queues**: This is where contacts wait before they are routed to and accepted by agents.
- **Agent queues**: These queues are created automatically when you add an agent to your contact center.

Contacts are only routed to agent queues when explicitly sent there as part of a flow. For example, you might route contacts to a specific agent who's responsible for certain customer issues, such as billing or premium support. Or you might use agent queues to route to an agent's voice-mail.

Contacts waiting in agent queues are higher priority than contacts waiting in standard queues. Contacts in agent queues have the highest priority and zero delay:

- **Highest priority**: If there's another contact in the basic queue, Amazon Connect chooses to give the agent the contact from the agent queue first.
- **Zero delay**: If the agent is available, the contact immediately gets routed to them.

**Queues in metrics reports**

In a [real-time metrics report](#), you can monitor how many contacts are in standard queues and agent queues. The following image shows a sample real-time metrics Queues report where an Agents table and Agent queues table have been added. It shows:

- **BasicQueue**, which is a standard queue. It shows one agent (John) is online.
- **Agents** table, which shows the agent John has set his CCP to **Available** and is ready to take contacts. A supervisor can change an agent's status from here. For example, set to **Offline**.
- **Agent queues** table, which shows John's agent queue. It shows John is online and can take contact from this queue, too.
When an agent gets a contact from a standard queue, the contact never appears in the agent queue. It just goes directly to the agent.

In a historical metrics report, by default agent queues don't appear in a Queues table. To show them, choose the Settings icon, then choose Show agent queues.
Tip

The metrics APIs don't support agent queues.

Default queue: BasicQueue

Amazon Connect includes a default queue named BasicQueue. Along with the default flows and default routing profile (named Basic routing profile), it powers your contact center so you don't need to do any customization. This is what enables you to get started quickly.

Concepts: Queues priority and delay

Priority and delay are powerful features that allow you to load balance contacts among groups of agents.
Example 1: Different priority but same delay

For example, one group of agents is assigned to a Sales routing profile. Since their primary job is sales, the Sales queue is Priority 1 and Delay is 0. But they can help with Support too, so that queue is Priority 2 and Delay is 0. This shown in the following table:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Priority</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Support</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

If there are no contacts in the Sales queue, then the agents will be presented with contacts from the Support queue.

Example 2: Same priority but different delay

Say you set the Support queue to Priority 1 and Delay of 30 seconds, as shown in the following table:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Priority</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Support</td>
<td>1</td>
<td>30</td>
</tr>
</tbody>
</table>

These agents will always get contacts from the Sales queue first because the delay is 0. However, when a contact in the Support queue ages past 30 seconds, it will also be treated as priority 1. The agents will then be presented with the contact from the Support queue.

Example 3: Different Priorities and Delays

Here’s a more complicated example for a Support routing profile:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Priority</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 Support</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Queue</td>
<td>Priority</td>
<td>Delay (in seconds)</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Tier 2 Support</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Tier 3 Support</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>Tier 4 Support</td>
<td>3</td>
<td>80</td>
</tr>
</tbody>
</table>

This routing profile prioritizes the Tier 1 Support and Tier 2 Support queues equally because each is priority 1.

- Agents may take contacts from the Tier 3 Support queue when:
  - Customers for Tier 3 Support are waiting for 20 seconds or longer.
  - And no contacts are in the Tier 1 Support or Tier 2 Support queues.
- Agents may take contacts from the Tier 4 Support queue when:
  - Customers in the Tier 4 Support queue have been waiting 80 seconds or longer.
  - And no contacts are in the Tier 1 Support, Tier 2 Support or Tier 3 Support queues.

**Priority takes precedence.** (You might think that agents take contacts from Tier 4 Support when contacts are in Tier 1 Support, Tier 2 Support, or Tier 3 Support and waiting 20 seconds or longer, but that's not right.)

**Example 4: Same Priority and Delay**

In this example a routing profile has only two queues, and they have the same priority and delay:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Priority</th>
<th>Delay (in seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Support</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

For this routing profile, the oldest contact is routed first. It goes to the agent who has been idle for the longest time.

For instructions on how to set priority and delay for a routing profile, see [Create a routing profile](#).
Concepts: Queue-based routing

In your business, you might want to route customers to specific agents based on certain criteria, such as the skill of the agent. This is called queue-based routing, also known as skills-based routing.

For example, an airline might have some agents who handle reservations for English-speaking customers, others who handle Spanish-speaking customers, and a third group that handles both types of customers, but only over the phone.

The following illustration shows you can:

• Assign the same routing profile to multiple agents.
• Assign multiple queues to a routing profile.
• Assign a queue to multiple routing profiles.

For an overview of the steps to set up queue-based routing, see Set up queue-based routing.

Concepts: Channels and concurrency

Agents can handle voice, chat, and tasks in Amazon Connect. When you set up a routing profile to handle multiple channels, you have two options:
• Option 1: Set up agents so they can handle contacts while already on another channel. This is called *cross-channel concurrency*.

• Option 2: Set up agents so they can be offered voice or chat or tasks if they are fully idle, depending on what is in queue. When you choose this option, after the agent starts work on contacts from one channel they will no longer be offered contacts from any other channels.

When using cross-channel concurrency, Amazon Connect checks which contact to offer the agent as follows:

1. It checks what contacts/channels the agent is currently handling.
2. Based on what channels they are currently handling, and the cross-channel configuration in the agent's routing profile, it determines whether the agent can be routed the next contact.
3. Amazon Connect prioritizes the longest waiting contact if Priority and Delay are equal. Even though it's evaluating multiple channels at the same time, First-In First-Out is still respected.

For a detailed example of how Amazon Connect routes contacts when cross-channel concurrency is set up, see *Example of how a contact is routed with cross-channel concurrency*.

To learn more about what the agent experiences in the Contact Control Panel when handling multiple chats, see *How to use the CCP to manage chats*.

**Concepts: Amazon Connect Flows**

A *flow* defines how a customer experiences your contact center from start to finish. At the most basic level, flows enable you to customize your IVR (interactive voice response) system.

For example, you can give customers a set of menu options and route customers to agents based on what they enter on their phone. Although with Amazon Connect, flows are significantly more powerful than that: you can create dynamic, personalized flows that interact with other AWS services.

**Default flows**

When you create an instance and claim a number, you automatically have a working contact center in just 5 minutes. This is because Amazon Connect includes a set of default flows that have already been published. It uses them to power your contact center.
When you customize your contact center and create new flows, you're replacing the default flows with your own.

For example, say you create a flow that includes putting the customer on hold.

- You can create a prompt to play while the customer is on hold, such as "Do your holiday shopping early this year. We're offering free shipping in November." And then play some music.

- If you don't create a prompt, Amazon Connect will play the Default customer hold flow automatically.

To see the list of default flows in the Amazon Connect console, go to Routing, Flows. They all start with Default in their name.

For a list of all the default flows and what they do, see Default flows.

Flow designer

To customize your contact center, you use the flow designer. It's a drag-and-drop interface that allows you to customize your contact center without any coding.

Flow blocks

Flow blocks are the building blocks of your flows. Each block is designed for a specific function a business might want in a contact center.

You configure a flow block by accessing its Properties page, as shown in the following GIF. After you drag the block onto the flow designer, click or tab the name of the block to access its properties page.
For a list of the available flow blocks and descriptions about what they do, see Flow block definitions.

Sample flows

To see how to put flow blocks together to create different flows, see Sample flows.
Best practices for Amazon Connect

This list of best practices can help you get the maximum benefit from Amazon Connect. These best practices are for flows, Lambda, chat, Amazon Lex, and the Contact Control Panel (CCP).

We also recommend reviewing Security Best Practices for Amazon Connect.

Flows

- Use consistent attribute naming conventions across all AWS services. Use camel case for yourAttributeNames to avoid confusion when passing and referencing variables.
- Use standard naming conventions for attribute names. Don't use spaces or special characters that could impact downstream reporting processes such as AWS Glue crawlers.
- Create modular flows. Make the flows as small as possible, and then combine modular flows into an end-to-end contact experience. This helps to keep your flows manageable, and you won't require numerous regression testing cycles.
- When you set User Defined or External values in dynamic attribute fields, use only alphanumeric characters (A-Z, 0–9) and periods. No other characters are allowed.
- Ensure all error branches are routed to a block that effectively handles the error or terminates the contact.
- Use a Set logging behavior block to enable or disable logging for segments of the flow where sensitive information is collected and can't be stored in CloudWatch.
- Use Set recording behavior block in your flow to disable and enable recordings according to your use case. Keep in mind that Amazon Connect records conversations with agents only. It doesn't record IVR interactions.
- Ensure that attributes used in the flow are set and referenced correctly. If there are periods prepended to the attribute names, you are likely using JSONPath ($) format while also selecting a variable type from the pick list. For example, using:
  - Save text as attribute and value $.External variableName works as expected.
  - Set dynamically and value variableName works as expected.
  - Set dynamically and $.External variableName results in a prepended period.
- Before transferring a call to agent and putting that call in a queue, ensure that Check hours of operation and Check staffing blocks are used. They verify that the call is within working hours and that agents are staffed to service.
• Ensure that callbacks are offered before and after queue transfer by using **Check queue status** blocks. Include a condition for **Queue capacity** that is greater than X, where X is a number representing your expected queue capacity.

• If queue capacity exceeds the expected capacity, use a **Get Customer Input** block to offer a callback. This retains the caller's position in the queue and calls them back when an agent is available.

• In the **Set callback number** block, choose the number to be used to call the customer back in the CCP. Use **System** and **Customer Number** or a new number, collected by a **Store Customer Input** block, using **System** and **Stored customer input**.

• Finally, add a **Transfer to queue** block. Configure it to **Transfer to callback queue** and configure the callback options to fit your specific use case.

• Use a **Loop prompts** block in your Customer queue flow to interrupt with a queued callback and external transfer option at regular intervals.

• Ensure that all countries referenced in external transfers or used for outbound dialing are added to the service quota for your account/instance.

• Ensure that all numbers referenced in external transfers are in E.164 format. Drop the national trunk prefix that you use when calling locally. This prefix would be the leading 0 for most of Europe, 1 for the US. The prefix is replaced by the country code. For example, the UK mobile number **07911 123456** in E.164 format is **+44 7911 123456** (tel:+447911123456).

• Ensure that there are no infinite loops in the flow logic. Also ensure that for each call, the flow connects the caller to an agent, bot, or transferred externally for further assistance.

**Lambda**

• Amazon Connect limits the duration of a sequence of Lambda functions to 20 seconds. It times out with an error message when the total execution time exceeds this threshold. Because customers hear silence while a Lambda function runs, we recommend adding a **Play prompt** block between functions to keep them engaged during the long interaction.

By breaking up a chain of Lambda functions with the **Play prompt** block, you can invoke multiple functions that last longer than the 20 second threshold.
Chat and Amazon Lex

- You can use the same bot for both the voice and chat channels. However, you may want the bot to respond differently based on the channel. For example, you want to return SSML for voice so a number is read as a phone number, but you want to return normal text to chat. You can do this by passing the Channel attribute. For instructions, see How to use the same bot for voice and chat.

- For voice, some words are best spelled phonetically to get the correct pronunciation, such as last names. If this is the case with your scenario, include it in the design of your bot. Or, you can keep the voice and chat bots separate.

- Tell agents about the bot. When a contact is connected to the agent, the agent sees the entire transcript in their window. The transcript includes text from both the customer and the bot.

Contact Control Panel

- If your agents use Google Chrome 71 to Chrome 75, and they use chat or tasks, add the CCP URL to the allowlist in the agent's Chrome settings. Otherwise, they won't hear the audio indicator notifying them that there's an incoming chat or task.

  For instructions, see this Google Chrome Help article.

Tutorials: An introduction to Amazon Connect

The tutorials in this section are provided to help you start using Amazon Connect. They show you how to set up your first instance, and test a sample voice and chat experience. Next, they show you how to set up an IT Help Desk contact center that uses the features in Amazon Lex.

These tutorials are suitable for both knowledge workers and developers.

Prerequisite

- An AWS account. If you don't already have one, create an account at: aws.amazon.com.

Print the tutorials

If you want to print the tutorials, choose the PDF icon at the top of any page, as shown in the following image.
What Is Amazon Connect?

Amazon Connect is an omnichannel cloud contact center. You can see customers.

A PDF version of the documentation opens. Press Ctrl+Home to return to the beginning of the PDF, then scroll down to the table of contents. Choose which pages to print.

Contents

- Tutorial 1: Set up your Amazon Connect instance
- Tutorial 2: Test the sample voice and chat experience
- Tutorial 3: Create an IT help desk

Tutorial 1: Set up your Amazon Connect instance

You can have multiple instances of Amazon Connect. Each instance contains all the resources related to your contact center, such as phone numbers, agent accounts, and queues.

In this tutorial, you open Amazon Connect, create an instance of Amazon Connect, and claim a phone number that you can use for testing.

Contents

- Step 1: Launch Amazon Connect
- Step 2: Create an instance
- Step 3: Claim a phone number

Step 1: Launch Amazon Connect

This step walks you through finding Amazon Connect in the AWS console, and opening the Amazon Connect console.

2. In the AWS Management Console, at the top of the page, choose the Services drop-down menu.

3. In the search box, type Amazon Connect.

4. Choose Amazon Connect.

   If this is the first time you've been to the Amazon Connect console, you'll see the following Welcome page.
5. Choose **Get started**.

**Congratulations!** You found and accessed Amazon Connect. You can use these same steps to search for and launch any AWS service.

Go to **Step 2: Create an instance**.

**Step 2: Create an instance**

1. On the **Amazon Connect virtual contact center instances** page, choose **Add an instance**.

2. On the **Set identity** page, in the **Access URL** box, type a unique name for your instance. For example, the following image shows **mytest10089** as a name. Choose a different name for your instance. Then choose **Next**.
3. On the Add administrator page, add a new administrator account for Amazon Connect. Use this account to log in to your instance later using the unique access URL. Choose Next.
a. The user name will be your Amazon Connect login. It's case sensitive.

b. The password must be between 8-64 characters, and must contain at least one uppercase letter, one lowercase letter, and one number.

4. On the **Set telephony** page, accept the default settings to allow incoming and outgoing calls. Choose **Next**.
5. On the **Data storage** page, accept the default settings and choose **Next**.

6. On the **Review and create** page, choose **Create instance**.
7. After the instance is created, choose **Get started**.
8. On the **Welcome to Amazon Connect** page, choose **Skip for now**.

9. You're now on the Amazon Connect dashboard. Your instance name (also called an **alias**) displays in the URL. On the left is the navigation menu.
Congratulations! You set up your instance and now you're on the Amazon Connect dashboard. Go to **Step 3: Claim a phone number**.

**Step 3: Claim a phone number**

In this step, you set up a phone number so that you can experiment with Amazon Connect.

1. On the Amazon Connect navigation menu, choose **Channels, Phone numbers**.
2. On the right side of the Manage Phone numbers page, choose Claim a number.

3. Select the DID (Direct Inward Dialing) tab. Use the drop-down arrow to choose your country/region. If you're in the US, you can specify the area code you want for your number, and only available numbers with that area code will be displayed. When numbers are returned, choose one.
4. Write down the phone number. You call it later in this tutorial.

5. In the **Description** box, type this note: **this number is for testing**.

6. In the **Flow / IVR** box, choose the drop-down arrow, and then choose **Sample inbound flow (first contact experience)**.

7. Choose **Save**.

**Congratulations!** You set up your instance and claimed a phone number. Now you're ready to experience how chat and voice work in Amazon Connect. Go to **Tutorial 2: Test the sample voice and chat experience**.
Tutorial 2: Test the sample voice and chat experience

To better understand what the voice and chat experiences are like for your agents and customers, you can test them without doing any development.

This tutorial shows you how to access and use the Contact Control Panel (CCP). The CCP is a web page that agents use to accept and manage voice and chat contacts.

Prerequisites

This tutorial is part of a series. If you performed Tutorial 1, you're ready to go. If not, here's what you need:

- An AWS account
- A configured Amazon Connect instance
- An Amazon Connect administrative account
- A claimed phone number

Contents

- Step 1: Handle a voice contact
- Step 2: Use the CCP to handle a chat contact

Step 1: Handle a voice contact

1. On the Amazon Connect navigation menu, choose Dashboard.
2. On the **Dashboard** page, choose **Test chat**.

3. On the **Test Chat** page, choose **Activate Contact Control Panel**.

4. If your browser prompts you to grant microphone access, choose **Allow**.

5. If your browser prompts you to allow notifications, choose **Allow**.

6. In the test CCP, set your status to **Available**.
7. Use your mobile phone to call the phone number that you claimed earlier. If you didn't write down the number, you can find it by going to Channels, Phone numbers.

8. When your call is joined to Amazon Connect you'll hear "Press 1 to be put in queue for an agent, 2 to ..." This is the Sample inbound flow that Amazon Connect runs by default. You're going to change this later in the tutorial.

9. You can play around with the different options in the Sample inbound flow. To connect to an agent, press 1, 1, 1.

10. In the CCP, choose Accept call.
11. You'll see what the CCP looks like when an agent is connected to a customer.

12. Choose **End call**.

Now the contact is in the After Contact Work (ACW) state. This is when the agent might enter some notes about the contact.
13. Choose **Close contact**. This frees the agent to take another incoming contact.

Well done! You've handled your first voice contact!

**Tip**

As an administrator, you can launch the CCP from anywhere on the Amazon Connect console by choosing the phone icon on the top of the page.

Next step

Go to [Step 2: Use the CCP to handle a chat contact](#) to experience how to handle a chat contact.
Step 2: Use the CCP to handle a chat contact

In Step 1, you used the Contact Control Panel (CCP) to manage a voice contact. In this step, you experience how to use the CCP to manage a chat contact.

1. This procedure assumes you've completed Step 1: Handle a voice contact. If you haven't, please do so now.

2. On the Test chat page, choose the chat bubble to start a chat.

3. The Sample inbound flow automatically transfers to you a queue. However, you can type a message as the customer and the agent receives it. For example, *I need help resetting my password*. 
4. In the CCP, accept the incoming chat.

5. Use the CCP to send chat messages to the customer.

6. When you're done chatting, choose **End chat**. Then in the CCP, choose **Close contact**.

Congratulations! You've experienced what it's like to chat using Amazon Connect.

Next, try Tutorial 3 to set up an IT Help Desk. It shows you how to set up routing, create a flow, and then test the custom voice and chat experience. Go to [Tutorial 3: Create an IT help desk](#).

**Tutorial 3: Create an IT help desk**

This tutorial shows you how to create an IT Help Desk. It shows how to create an Amazon Lex bot that finds out why the customer is calling. You next create a flow to use the customer's input to route them to the right queue.

**Prerequisite**

This tutorial is part of a series. If you performed Tutorial 1, you're ready to go. If not, here's what you need:

- An AWS account
- A configured Amazon Connect instance
- An Amazon Connect administrative account
- A claimed phone number
Step 1: Create an Amazon Lex bot

Bots provide an efficient way to offload repetitive tasks from your agents. This tutorial shows how to use the bot to find out why customers are calling the IT Help Desk. Later, we use the customer's response to route them to the right queue.

In previous tutorials, you used the Amazon Connect console. In this tutorial to set up a bot, you use the Amazon Lex console.

This step has five parts to it.

Contents

- Part 1: Create an Amazon Lex bot
- Part 2: Add intents to your Amazon Lex bot
- Part 3: Build and test the Amazon Lex bot

Part 1: Create an Amazon Lex bot

This step assumes it's the first time you've opened the Amazon Lex console. If you've created an Amazon Lex bot before, your steps differ slightly from the ones in this section.

1. Choose the following link to open the Amazon Lex console, or enter the URL in your web browser: https://console.aws.amazon.com/lex/.

2. If this is the first time you've created Amazon Lex bot, choose Get Started. Otherwise, you're already in the Amazon Lex dashboard.
3. Choose **Create a blank bot**.

4. Enter the following information:
   - **Bot name** — For this tutorial, name the bot **HelpDesk**.
   - **IAM permissions**: Choose **Create a role with basic Amazon Lex permissions**.
• **COPPA**— Choose whether the bot is subject to the [Children's Online Privacy Protection Act](https://www.copps.org/).  

• **Idle session timeout**— Choose how long the bot should wait to get input from a caller before ending the session.

5. Choose *Next*.

6. On the *Add language to bot* page, choose the language and voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joanna.

7. Choose *Done*.

Go to [Part 2: Add intents to your Amazon Lex bot](#).
Part 2: Add intents to your Amazon Lex bot

An intent is the action the user wants to perform. In this part, add two intents to the bot. Each intent represents a reason that users call the Help Desk: password reset and network issues.

1. In the Amazon Lex console, in the **Intent details** section, enter **PasswordReset** as the name of your intent.

2. Scroll to the **Sample utterances** section.
3. Type **I forgot my password**, and then choose **Add utterance**. Then add **reset my password** and choose **Add utterance** again.

4. Choose **Save intent**.

5. On the left navigation menu, choose **All intents list**.

6. On the left navigation menu, choose **Back to intents list**.
7. Choose Add intent, Add empty intent, and assign the name NetworkIssue. Scroll down the page and add the following sample utterances:

- I can't access the internet
- my email is down

When you're done, go to Part 3: Build and test the Amazon Lex bot.

Part 3: Build and test the Amazon Lex bot

Build and test your bot to make sure that it works as intended before you publish it.

1. In the Amazon Lex console, choose Build. The build may take a minute or two.

2. When it's finished building, choose Test.

3. Test the PasswordReset intent. In the Test Draft version pane, type I forgot my password, and press Enter.
4. The verification looks like what's shown in the following image.

5. To confirm that the `NetworkIssue` intent is working, type **my email is down**. The verification looks like what's shown in the following image.
Go to Step 2: Add permissions to Amazon Lex bot.

**Step 2: Add permissions to Amazon Lex bot**

To use a bot in your flow, add it to your Amazon Connect instance.

1. Open the Amazon Connect console (https://console.aws.amazon.com/connect/).
2. Choose the name of the instance that you created.
3. Do not log in on the name page (this method of logging in is for emergency access only). Rather, choose Flows.
4. Under **Amazon Lex**, use the drop-down arrow to choose **HelpDesk**. Under **Alias**, choose **TestBotAlias**, and then choose **+ Add Lex Bot**, and then choose **Add Amazon Lex Bot**.

5. When you're done, choose Amazon Connect to navigate back to instances page.

6. Choose the access URL of your instance.
The **Access URL** takes you back to the Amazon Connect dashboard.

**Step 3: Set up routing**

In this step, you start at the Amazon Connect console for your instance. This step shows how to set up your queues, create a routing profile, and then assign your user account to the profile.

1. On the navigation menu, go to **Routing, Queues**.

2. Choose **Add queue**.
3. Complete the **Add queue** page, as shown in the following image, to add a queue named **PasswordReset**. When done, choose **Save**.

The following image shows the **Settings** section of the **Add queue** page. Add your default caller ID name and outbound caller ID number.
Settings

Outbound caller configuration
Set the default caller ID name that will display to customers. Learn more.

<table>
<thead>
<tr>
<th>Default caller ID name</th>
<th>Outbound caller ID number</th>
<th>Outbound whisper flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Callback ID name</td>
<td>Search for phone numbers</td>
<td>Search for contact flow</td>
</tr>
<tr>
<td>Example Corp</td>
<td>+1 503-922-7089</td>
<td></td>
</tr>
</tbody>
</table>

For the purposes of this tutorial, leave the following empty: Outbound whisper flow, Quick connect, and Maximum contact in queue.

4. Add a queue named NetworkIssue. Complete the Add queue page like you did for the PasswordReset queue.

When done, you'll have three queues.

5. On the navigation menu, go to Users, Routing Profiles.
6. Choose **Add routing profile**.

7. Assign a name to the new profile (for example, **Test routing profile**). Enter a description, select **Voice**, **Chat**, and set **Maximum chats** to 1.
8. In the Queues section, use the drop-down arrow to search for the queues you just created. Choose NetworkIssue, select Voice and Chat. Choose Add Queue.

9. Add the PasswordReset queue. Select Voice and Chat, and then choose Save.

10. Under Default outbound queue, use the drop-down arrow to choose BasicQueue.

11. When done, scroll to the top of the page, and choose Save to save the profile.
12. On the navigation menu, go to Users, User management.

13. On the User management page, select your login name.

14. On the Edit page, in the Settings section, in the Routing profile dropdown menu, choose the routing profile you created, for example, Test routing profile. Choose Save.

Routing is all set up and ready to go.
Step 4: Create a flow

Although Amazon Connect comes with a set of built-in flows, you can create your own flows to determine how a customer experiences your contact center. The flows contain the prompts that customers hear or see, and they transfer them to the right queue or agent, among other things.

In this step, create a flow that's specific to the IT Help Desk experience that you're creating.

1. On the Amazon Connect navigation menu, go to Routing, Flows.

2. Choose Create flow.

3. The flow designer opens. Enter a name for the flow, such as Test flow.
4. Use the search box to search for the following block, and drag them onto the grid: **Set logging behavior**, **Set voice**, and **Play prompt**.

5. Use your mouse to drag an arrow from the **Entry** block to the **Set logging behavior** block.

6. Connect the remaining blocks, as shown in the following image.
7. Choose the **Play prompt** title to open its properties page.

8. Configure the **Play prompt** block, as shown in the following image, and then choose **Save**. Choose **Text-to-speech or chat text**, choose **Set manually**, enter *Welcome to the IT Help desk*. 
9. Add a Get customer input block and connect to the Play prompt block.

10. Choose the title of the Get customer input block to open the properties page.
11. Configure the **Get customer input** block, as shown in the following images. Choose **Text-to-speech or chat text**, **Set manually**, and enter *How can I help* in the text box. Set the **Interpret as** dropdown box to **Text**.

![Get customer input block](image1)

The following image shows the Amazon Lex tab. Choose the name of your Amazon Lex bot from the dropdown list. For **Alias** enter **$LATEST**.

![Amazon Lex tab](image2)

12. While still in the **Get customer input** block, choose **Add an intent**.
13. Enter the names of the intents that you created in the Amazon Lex bot, such as PasswordReset and NetworkIssue. They are case sensitive!

14. Choose **Save**.

15. Add a **Play prompt** block and connect it to the **PasswordReset** branch.

16. Choose the **Play prompt** title to open its properties page. Configure the **Play prompt** block with the message *We're putting you in a queue to help you with password reset*. Choose **Save**.

17. Add a second **Play prompt** block and connect it to the **NetworkIssue** branch.

18. Choose the **Play prompt** title to open its properties page. Configure the **Play prompt** block with the message *We're putting you in a queue to help you with your network issues*. Choose **Save**.

19. Add a **Disconnect / hang up** block to the grid. Connect the **Default** and **Error** branches to it.

20. Add a **Set working queue** block to the grid. Connect the **Play prompt** block for PasswordReset.
21. Choose the Set working queue title to open its properties page. Configure the Set working queue block by using the drop-down arrow to choose the PasswordReset queue. Choose Save.

22. Add a Set working queue block for NetworkIssue, and configure it with the NetworkIssue queue.
23. Drag two **Transfer to queue** blocks (from the **Terminate/Transfer** group) onto the grid.

24. Connect each of the **Set working queue** blocks to a **Transfer to queue** block.

25. Drag another **Disconnect/hang up** block onto the grid. Connect all of the remaining **Error** and **At capacity** branches to it.

26. The completed flow looks similar to the following image.

27. Choose **Save**, and then choose **Publish**.
Tip

Any blocks that aren't connected or configured correctly generate an error. If this happens, double-check that all branches are connected.

28. When the flow publishes, it displays the message that it saved successfully.

If the flow doesn't save, double-check that all the branches are connected to blocks. That's the most common reason flows don't publish.

Step 5: Assign the contact flow to the phone number

1. On the navigation menu, go to Channels, Phone Numbers.
2. On the Manage Phone numbers page, choose your phone number.
3. Use the drop-down box to choose the flow you just created, and then choose `Save`.

Everything is all set up! Now you're ready to test your IT Help Desk. Continue on to `Step 6: Test a custom voice and chat experience`. 
Step 6: Test a custom voice and chat experience

You're ready to try out the Amazon Lex bot, routing, and flow. The first step is to tell Amazon Connect which flow you want to test.

1. On the navigation menu, go to the Dashboard and choose Test chat.

2. Choose Test Settings.

3. Use the drop-down box to choose the flow you created, for example, Test flow. Choose Apply.

Test a custom chat experience

1. If needed, choose the chat bubble to start a chat.
2. Amazon Connect automatically detects a contact and runs the flow that you created. It displays messages from the flow.

3. Enter that you need help resetting a password. Then accept the incoming chat. The following image shows you what the chat and agent interfaces look like when you're trying them.
4. In the customer pane on the right, choose **End chat** to close the chat window.

5. In the test CCP, choose **Close contact** to end the After Contact Work (ACW).

**Test a custom voice experience**

1. If the test chat window is still open, choose **End chat** to close it. Then you can try the voice experience.

2. Call your phone number.

3. When prompted, say *I'm having trouble accessing the internet*. You should hear the message that you're being transferred to the NetworkIssue queue.

4. Switch to the test CCP and accept the incoming call.

**Tip**

After you're transferred, you'll hear this message:

*Thank you for calling. Your call is very important to us and will be answered in the order it was received.*

This message is generated by a [default flow](#) named [Default customer queue](#).
5. After you accept the call, but before you're connected to the customer, you'll hear an inbound whisper stating what queue the contact is in, for example, NetworkIssue. This helps you know what the customer is calling about.

   The inbound whisper is generated by a default flow named Default agent whisper.

6. When done, end the call.

7. In the CCP, choose Clear contact to end After Contact Work (ACW).

Congratulations! You built and tested an omnichannel IT Help Desk that leverages Amazon Lex and offers customers both chat and voice.

Tip
If you don't want to keep the phone number that you claimed for testing, you can release it back to inventory. For instructions, see Release a phone number from Amazon Connect back to inventory.

Ensure call quality: Design your contact center for low latency

Note
As of July 2023 we have simplified requirements to claim phone numbers that are located in countries outside of the AWS Region where your Amazon Connect instance is located. The process has been simplified to remove the need for the opt-in approval. Instead we provide best practice design guidance. This makes it easier for you to use an Amazon Connect instance that is created in the US-East Region, for example, and then request numbers in Japan. Or, if your instance is created in Asia Pacific (Singapore), you don't need to contact AWS Support to claim phone numbers based in Europe or US Regions. We continue to extend the support of Amazon Connect so you can claim phone numbers in the countries you need, wherever you need them.

If you are configuring your Amazon Connect instance to support phone numbers outside of your country's home AWS Region, we recommend the following best practices.
1. Anchor either your phone numbers or agents in the same AWS Region where they are geographically located. For example, if your agents are located in a US Region, your Amazon Connect instance should be created in an AWS Region in the US, too. Or, if your phone numbers are in an EU country, your Amazon Connect instance should be created in an EU AWS Region, too.

   a. If both your phone numbers and agents are located in an AWS Region that is different from the one where your Amazon Connect instance is created, call latency is extended above 500ms. This latency may result in call quality issues.

2. Calculate your latency before setting up your Amazon Connect contact center in production. Perform the following steps on a test environment:

   a. Use the Amazon Connect Endpoint Test Utility to check latency.

   b. Calculate the latency for routing telephony from the country to the AWS Region using internet-based, external tools, such as WonderNetwork.

   c. For calls with the best call quality, we recommend configurations with less than 500ms of latency end-to-end.

   d. You may determine that call quality is acceptable at up to 900ms of latency. However, if you note a call-quality issue that can be due to latency, and other potential causes are ruled out (for example, neither packet loss nor jitter are detected), we recommend configuring your Amazon Connect instance or telephony for a lower latency. For example, create your Amazon Connect instance in the same Region as your telephony or agents.

   **Important**

   When call latency is greater than 900ms, it leads to a significant delay between agents and customers.

3. Check that latency matches your design.

   After you claim a number you can immediately call it to hear what the experience will be like for your customers. Amazon Connect uses the default flows to power your initial experience.

   To test a customized flow, assign a phone number to it and then call that number.
Architectural guidance for Amazon Connect

This topic provides guidance and best practices for designing and building reliable, secure, efficient, and cost-effective systems for your Amazon Connect contact center workloads. Using this guidance can help you build stable and efficient workloads, allowing you to focus on innovation, reduce costs, and improve your customer's experience.

This content is intended for chief technology officers (CTOs), architects, developers, and operations team members.

Contents

- Amazon Connect workload layers
- Scenario and deployment approaches
- Operational Excellence
- Security: Design principles for developing a secure contact center
- Reliability
- Performance efficiency
- Cost optimization

Amazon Connect workload layers

You can separate Amazon Connect workloads into the following layers: telephony, Amazon Connect interface/API, flows/IVR, agent workstation, and metric and reporting.

Telephony

Amazon Connect is integrated with multiple telephony providers with redundant dedicated network paths to three or more Availability Zones in every Region where the service is offered today. Capacity, platform resiliency, and scaling are handled as part of the managed service,
allowing you to efficiently ramp from 10 to 10,000+ agents without worrying about the management or configuration of underlying platform and telephony infrastructure. Workloads are load balanced across a fleet of telephony media servers, allowing new updates and features to be delivered to you with no downtime required for maintenance or upgrades. If a particular component, data center, or an entire Availability Zone experiences failure, the affected endpoint is taken out of rotation, allowing you to continue to provide a consistent quality experience for your customers.

When a voice call is placed to an Amazon Connect instance, the telephony layer is responsible for controlling the endpoint that your customer calls into through their carrier, across the PSTN and into Amazon Connect. This layer represents the audio path established between Amazon
Connect and the customer. Through the Amazon Connect interface layer, you can configure things like outbound caller ID, assign flow/IVRs to phone numbers, enable live media streaming, enable call recording, and the ability to claim phone numbers without any prior traditional telephony knowledge or experience. Additionally, when migrating workloads to Amazon Connect, you have the option to port your existing phone numbers by opening a support case in your AWS Management Console. You can also forward your existing phone numbers to numbers that you've claimed in your Amazon Connect instance until you are fully migrated.

Amazon Connect Interface/API

The Amazon Connect interface layer is the access point that your agents and contact center supervisors and administrators will use to access Amazon Connect components like reporting and metrics, user configuration, call recordings, and the Contact Control Panel (CCP). This is also the layer responsible for:

- Single Sign-On (SSO) integration user authentication
- Custom desktop applications created using the Amazon Connect Streams API that may provide additional functionality and/or integrate with existing Customer Relationship Management (CRM) systems including the Amazon Connect Salesforce CTI Adapter.
- Amazon Connect contact-facing chat interface
- Chat web server hosting the Amazon Connect Chat API
- Any Amazon API Gateway endpoints and corresponding AWS Lambda functions necessary to route chat contacts to Amazon Connect.

Anything your agents, managers, supervisors, or contacts use to access, configure, or manage Amazon Connect components from a web browser or API is considered the Amazon Connect interface layer.
Flow / IVR

The Flow/IVR layer is the primary architectural vehicle for Amazon Connect and serves as the point of entry and first line of communication with customers reaching out to your contact center. After a customer contacts your Amazon Connect instance, a flow controls the interaction between Amazon Connect, the contact, and the agent, allowing you to:

- Dynamically invoke AWS Lambda functions to make API calls.
- Send real-time IVR and voice data to third-party endpoints through Amazon Kinesis.
- Access resources inside your VPC and behind your VPN.
- Call other AWS services like Amazon Pinpoint to send SMS messages from the IVR.
- Perform data dips to database like Amazon DynamoDB to service your contacts.
- Call Amazon Lex directly from the flow to invoke a Lex bot for Natural Language Understanding (NLU) and Automatic Speech Recognition (ASR).
• Play dynamic and natural Text-to-Speech through Amazon Polly, and use SSML and Neural Text-to-Speech (NTTS) to achieve the most natural and human-like text-to-speech voices possible.

Flows enable you to dynamically prompt contacts, collect and store contact attributes, and route appropriately. You can assign a flow to multiple phone numbers, and manage and configure it through Amazon Connect.

Agent workstation

The agent workstation layer is not managed by AWS. It consists of any physical equipment and third-party technologies, services, and endpoints that facilitate your agent’s voice, data, and access the Amazon Connect interface layer. Components in the agent workstation layer include:

• The Contact Control Panel (CCP) agent hardware
• Network path
• Agent headset or handset
• VDI environment
• Operating system and web browser
• Endpoint security
- All networking components and infrastructure
- Internet Service Provider (ISP) or AWS Direct Connect dedicated network path to AWS.
- All other aspects of your agent's operating environment including power, facilities, security, and ambient noise.

**Metric and reporting**

The metric and reporting layer includes the components responsible for delivering, consuming, monitoring, alerting, or processing real-time and historical metrics for your agents, contacts, and contact center. This includes all native and third-party components responsible for facilitating the processing, transmission, storage, retrieval, and visualization of real-time or historical contact center metrics, activity audit, and monitoring data. For example:

- Call recordings and scheduled reports stored in Amazon Simple Storage Service (Amazon S3).
• Contact records that you can export to AWS database services like Amazon Redshift or your own on-premises data warehouse with Amazon Kinesis.
• Real-time dashboards you create with Amazon OpenSearch Service and Kibana.
• Amazon CloudWatch metrics generated that you can use to set alarms based on static thresholds, set up Amazon SNS notifications to alert to your administrators and supervisors, or launch AWS Lambda functions in response to the event.

Scenario and deployment approaches

Amazon Connect offers self-service configuration and enables dynamic, personal, and natural customer engagement at any scale with a variety of migration and integration options. In this section, we explain the following scenarios and deployment approaches to consider when designing a workload for Amazon Connect:

• Traditional contact center
• Inbound
• Outbound
• Hybrid contact center
• Legacy contact center migration
• Virtual desktop infrastructure (VDI)

**Traditional contact center**

The traditional contact center requires a significant telephony, media, networking, database, and compute infrastructure footprint that can span multiple vendors and data center locations to service contacts. Each individual solution and vendor have unique hardware, software, networking, and architectural requirements that have to be met while resolving versioning, compatibility, and licensing conflicts.

It is common to have separate vendors and infrastructure requirements for local and remote agent hardware and VPN connectivity, Text-To-Speech (TTS), Automatic Call Distribution (ACD), Interactive Voice Response (IVR), voice audio and data, physical desk phones, voice recording, voice transcriptions, chat, reporting, database, Computer Telephony Integration (CTI), Automatic Speech Recognition (ASR), and Natural Language Understanding (NLP). Your contact center architecture and infrastructure becomes more complicated when you consider multi-stage development, quality assurance, and test environments.
A typical Amazon Connect deployment solves or reduces many of the challenges associated with versioning, compatibility, licensing, contact center telephony infrastructure, and maintenance. It gives you the flexibility to create instances in new locations in minutes and migrate components individually, or in parallel, to best meet your individual business objectives. You can use flows for your IVR/ACD, have voice and data delivered through a supported web browser to your agent’s softphone, port your existing phone numbers, redirect softphone audio to an existing desk phone, invoke an Amazon Lex bot natively within your flow for ASR and NLP, and use the same flow for chat and voice. You can use Amazon Contact Lens to automatically generate voice transcriptions, perform key word identification and sentiment analysis, and categorize contacts. For agent CTI
data and real-time voice streaming, you can use Amazon Connect Agent Event Streams and Kinesis Video Streams. You can also create multi-stage development, quality assurance, and test environments at no additional cost and only pay for what you use.

**Inbound**

Inbound is a contact center term used to describe a communication request initiated by a contact to the center. Contacts can reach your Amazon Connect instance for inbound self-service or to speak with a live agent in a variety of ways, including voice and chat. Voice contacts go through the PSTN and are routed to the Amazon Connect Instance telephony entry point through the phone number claimed in your instance. You can reserve a phone number with Amazon Connect directly, port your existing phone number, or forward voice contacts to Amazon Connect. Amazon Connect can provide local and toll-free numbers in all Regions where the service is supported.
When a phone call is placed to a number claimed in or ported to your Amazon Connect instance, the flow associated with the called number will be invoked. You can define the flow using flow blocks that can be configured with no coding knowledge required. The flow determines how the contact should be processed and routed, optionally prompting the contact for additional information to assist in routing decisions, storing those attributes to the contact details, and, if necessary, routing that contact to an agent with all of the call details and transcripts gathered along the way. Through the flow, you can invoke AWS Lambda functions to query customer information, call other AWS services like Amazon Pinpoint to send SMS text messages, and use native AWS service integrations including Amazon Lex for NLU/NLP and Kinesis Video Streams for real-time streaming of voice calls.
If an inbound contact needs to reach an agent, the contact is put into a queue and routed to an agent when they change their status to Available, according to your routing configuration. When the available agent’s contact is accepted manually or through auto-accept configuration, Amazon Connect connects the contact with the agent.

When an inbound contact comes from a browser or mobile app request for a chat session, the request is routed to a web service or Amazon API Gateway endpoint that calls the Amazon Connect chat API to invoke the flow configured in your request. You can use the same flows for chat and voice, where the experience is managed and routed dynamically, based on the logic defined in the flow.
Outbound

Amazon Connect allows you the ability to programmatically make outbound contact attempts to local and international endpoints, reduce agent set-up time between contacts, and improve agent productivity. By using the Amazon Connect Streams API and StartOutboundVoiceContact, you can develop your own outbound solution or take advantage of existing partner integrations that work with your CRM data to create dynamic, personalized experiences for your contacts and empowering your agents with the tools and resources they need to service those contacts.

Outbound campaigns are typically driven by contact data exported from CRMs and separated into contact lists. Those contacts are prioritized and either delivered to the agents to initiate after a period of preview or programmatically contacted using the Amazon Connect Outbound API, driven by your flow logic, and connecting to agents as needed. Typical outbound contact center use cases include fraud and service alerts, collections, and appointment confirmations.

Hybrid

If you have requirements to transfer contacts between Amazon Connect and legacy contact center technologies, you can use a Hybrid model architecture to pass contact data with the transfer. For example, a sales business unit on a legacy contact center platform may need to transfer a call to the service business unit that’s been migrated to Amazon Connect. Without a Hybrid architecture, call details will be lost and may require the contact to repeat information. This could increase handle times and may result in contact calling again for the same purpose.

Hybrid architectures require you to claim as many phone numbers as your expected maximum concurrent contacts and an intermediary state database accessible by both Amazon Connect and your legacy contact center platform. When a transfer is required to the other platform, you will use one of these phone numbers as a unique identifier, flag it as in-use in your intermediary database, insert your contact details, and use that number as your ANI or DNIS when you transfer the contact. When the contact is received by the other contact center platform, you will query the intermediary database for the contact details based on the unique ANI or DNIS you used. Hybrid architectures are typically used as an interim migration step because of the additional cost and complexity associated.

IVR-only

You may choose to use Amazon Connect to drive the contact’s IVR experience while your agent population remains on your legacy contact center platform. With this approach, you can use
Amazon Connect flows to drive self-service and routing logic, and, if necessary, transfer the contact to the target agent or agent queue on your legacy contact center platform.

In this diagram, the contact dials a phone number claimed in your Amazon Connect instance for service. If they need to be transferred to an agent on your legacy contact center platform, an AWS Lambda function is invoked to query an available unique phone number, flag it as in-use, and write relevant contact details to an intermediary database. The contact is then transferred to the legacy contact center platform with the phone number returned from the Lambda function. The legacy contact center will then perform a query on the intermediary database for the contact details, route accordingly, and reset the contact data in the intermediary database, allowing the phone number to be used again.
Agent-only

With this approach, your legacy contact center IVR drives the contact’s IVR self-serve and routing logic, and, if necessary, transfers the contact to Amazon Connect to route to your agent population.

In this diagram, the contact dials a phone number claimed with your legacy contact center platform. If they need to be transferred to an agent on Amazon Connect, the legacy contact center platform will query an available unique phone number, flag it as in-use, and write relevant contact details to an intermediary database. The contact will then be transferred to Amazon Connect with the phone number returned by the legacy contact center’s query. Amazon Connect will then query the contact details from the intermediary database using AWS Lambda, route accordingly, and reset the contact data in the intermediary database, allowing the phone number to be used again.
Mixed

In this scenario, you may have your IVR and agents operating in parallel on Amazon Connect and your legacy contact center platform to allow for site, agent group, or line-of-business migrations.

Legacy contact center migration

When you are evaluating Amazon Connect for new or existing workloads, there are several strategies you can consider. For situations that require contact details to be included when contacts are transferred between Amazon Connect and your legacy contact center solution, a Hybrid model architecture will be required until the migration is complete. The approaches described in this section allow you to move specific lines of business in phases, manage training and support, and mitigate risks associated with change.
New workload

You may decrease risk associated with changes to existing business units and increase flexibility and digital innovation potential by adopting a net new workload on Amazon Connect. Net new workloads that do not require the Hybrid model architecture are less complex, are not affected by change in business process or agent routine, and have a faster time to market. Adopting a net new workload allows you to take advantage of usage-based, pay-as-you-go pricing. Your contact center resources are available to create a new experience for their end users, test and implement it to evaluate the platform, gain confidence, and build the skills and operational mechanisms to prepare for larger migration across existing workloads.

IVR First

You may choose to use Amazon Connect to drive the contact’s IVR experience while your agent population remains on your legacy contact center platform. With this approach, you can use Amazon Connect Flows to drive self-service and routing logic, and, if necessary, transfer the contact to the target agent or agent queue on your legacy contact center platform.

IVR Last

With this approach, your legacy contact center IVR drives the contact’s IVR self-serve and routing logic, and, if necessary, transfers the contact to Amazon Connect to route to your agent population.

Line of business segmentation

If your lines of business have separate IVRs or don’t require contact transfers to legacy contact center platforms, you may want to consider a line of business migration approach. For example, selecting your service desk for internal support as your first line of business to migrate. After migrating your service desk IVR and agent population to Amazon Connect, you may choose to forward your existing contact to Amazon Connect, porting the endpoint after testing and business validation is completed.

Site or agent group segmentation

If your contact center has a global footprint, services contacts from multiple countries, or is managed independently by a respective geography or location, you may want to consider a migration approach based on a physical site or geography of agents. Each agent population and/or geography can have its own unique requirements and considerations that may not apply globally.
Approaching your migration this way will allow each site or agent group to gain the skills they need to continue to operate independently before moving onto the next.

**Virtual desktop infrastructure (VDI)**

While you can use the Amazon Connect Contact Control Panel (CCP) within Virtual Desktop Infrastructure (VDI) environments, it will add another layer of complexity to your solution that warrants separate POC efforts and performance testing to optimize. The configuration/support/optimization is best handled by your VDI support team and the following deployment models are the most commonly implemented.

**VDI client with local browser access**

You can build a custom CCP with the Amazon Connect Streams API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. The following diagram describes that approach:

![Diagram of VDI client with local browser access](image)

**VDI client without local browser access**

Sometimes the VDI client does not have access to a local browser. In this scenario, you can create a single CCP instance with media run from the VDI server allowing access to enterprise resources. For this deployment model UDP audio is usually enabled on the VDI OS. This deployment model requires extensive testing to calibrate the different VDI server parameters to optimize quality of experience:
Operational Excellence

Operational excellence includes the ability to run and monitor systems to deliver business value and continually improve supporting processes and procedures. This section consists of design principles, best practices, and questions surrounding the operational excellence of Amazon Connect workloads.

Prepare

Consider the following areas to prepare for an Amazon Connect workload.

AWS account

With AWS Organizations, you can set up multiple AWS accounts for each level of your development, staging, and quality assurance environments. This allows you to centrally govern your environment as you grow and scale your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to centrally manage billing; control access,
compliance, and security; and share resources across your AWS accounts. This is the starting point for consuming AWS services along with a cloud adoption framework.

Region selection

Amazon Connect Region selection is contingent upon data governance requirements, use case, services available in each Region, telephony costs in each region, and latency in relation to your agents, contacts, and external transfer endpoint geography.

Telephony

- **Phone number porting** Open a porting request as far in advance of your pending go-live date as possible.

  When porting phone numbers for critical workloads, include all requirements and use case information in your claim/port number several months before the go-live date. This includes requests for live cutover support, communication prior, during, and after cutover, monitoring, and anything else specific to your use case.

  For detailed information about porting your numbers, see [Port your current phone number to Amazon Connect](#).

- **Carrier diversity** In the US, you should use Amazon Connect telephony services for US toll-free numbers, allowing you to route toll-free traffic across multiple suppliers in an active-active fashion at no additional charge. In situations where you are forwarding inbound traffic to an Amazon Connect phone number, you should request redundant DID or Toll-Free numbers across multiple telephony providers. If you are claiming or porting multiple DID or Toll-Free numbers outside of the US, you should request that those numbers be claimed or ported to a variety of telephony providers for increased resiliency.

- **International toll-free and high-concurrency DIDs** If you are using an existing toll-free national service to redirect inbound traffic to DIDs, you should request DID phone numbers across multiple telephony providers. A general recommendation for this configuration is 100 sessions per-DID and your AWS Solutions Architect can help with capacity calculations and setup.

- **Testing** Thoroughly test all use case scenarios, preferably using the same or similar environment as your agents and customers. Ensure that you test several inbound and outbound scenarios for quality of experience, Caller ID functionality, and measure latency to ensure it falls within acceptable range for your use case. Any deviations from your target agent and customer environments need to be measured and accounted for. For more information, including use case testing instructions and criteria, see [Troubleshooting Issues with the Contact Control Panel (CCP)](#).
Agent workstation

The Amazon Connect Call Control Panel (CCP) has specific network and hardware requirements that must be met to ensure the highest quality of service for your agents and contacts:

- Set Up Your Network for CCP use and ensure that your agent hardware meets minimum requirements.
- Ensure that you have used the Amazon Connect Check Amazon Connectivity Tool on the same network segment as your agents to verify that your network and environment is configured correctly for CCP use.
- Calculate PSTN latency for use cases that require agents and contacts to be in geographically distant locations
- Review the Troubleshooting Issues with the Contact Control Panel (CCP) section to create runbooks and playbooks for your agents and supervisors to follow should they encounter issues.
- Set up monitoring for your agent workstations and consider partner solutions for call quality monitoring. Your goal with monitoring your agent workstations should be the ability to identify the source of any potential network and resource contention. For example, consider a typical agent's softphone network connection path to Amazon Connect:
Without setting up monitoring at the local LAN/WAN, path to AWS, and agent workstation levels, it’s difficult and often impossible to determine if a voice quality issue is originating from your agent’s workstation, their private LAN/WAN, ISP, AWS, or the contact itself. Setting up logging and alerting mechanisms proactively is critical in determining root cause and optimizing your environment for voice quality.

**Configure your existing directory**

If you are already using an AWS Directory Service directory to manage users, you can use the same directory to manage user accounts in Amazon Connect. This must be decided and configured when you create your Amazon Connect instance. You cannot change the identity option you select after you create the instance. For example, if you decide to change the directory you selected to enable
Single Sign On (SSO) for your instance, you can delete the instance and create a new one. When you delete an instance, you lose all configuration settings and metrics data for it.

**Service Quotas**

Review the default service quotas for each service involved in your workload as well as the default service quotas for Amazon Connect and request increases where applicable. When requesting an increase for Amazon Connect, be sure to use expected values without additional padding for fluctuations. Fluctuations are considered automatically when you make your request.

**AWS Enterprise support**

AWS Enterprise Support is recommended for business and/or mission-critical workloads on AWS. Both Enterprise Support and Well-Architected Review with an AWS Solutions Architect are required to qualify for the Amazon Connect Service Level Agreement.

**AWS well-architected review**

Before any migration or implementation to Amazon Connect, follow our best practices by using the AWS Well-Architected Framework, Operational Excellence. The Framework provides a consistent approach for you to evaluate architectures and implement designs that will scale over time based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization. We also recommend using AWS Enterprise Support for business and mission-critical workloads in AWS. Both Enterprise Support and Well-Architected Review with your AWS Solutions Architect are required to qualify for the Amazon Connect Service Level Agreement.

**Operate**

Consider the following areas to operate an Amazon Connect workload.

**Logging and monitoring**

See [Monitoring your instance using CloudWatch](#) and [Logging Amazon Connect API calls with AWS CloudTrail](#).

**Contact attributes**

Amazon Connect allows you to dynamically set and reference contact attributes within flows to create dynamic and personalized experiences for your contacts, create powerful self-service applications, data-driven IVRs, integrations with other AWS services, simplify phone number
management, and allows for custom real-time and historical reporting and analytics. The following are Best practices and considerations you can follow to reduce complexity, prevent data loss, and ensure a consistent quality of experience for your contacts.

Note the following considerations:

- **Data size** – To prevent truncation, the size limitation for contact attributes you can set in a Set contact attributes block varies depending on the charset, encoding, and language used. While this is generally enough data to play a short story for a contact, it is possible to exceed this limit, truncating any attributes set over the 32KB.

- **Data sensitivity** – Note if any attributes being set, queried, and referenced are sensitive or fall under any regulatory guidelines and ensure that the data is being treated appropriately for your use case.

- **Data persistence** – Any attributes set using the Set contact attributes block will be included in the contact record for your contact and available for screen pop to any custom agent desktop using the Streams API. Any time the attribute is referenced within your flow and logging is enabled for the flow, the name and value of the attribute will be logged to Amazon CloudWatch.

**Best practices**

- **Monitor usage** – As you implement new functionality, onboard new business units, and iterate on existing flows, look up your current attribute usage in contact search, copy the attributes to a text editor, add the new attributes, and ensure that you do not exceed the 32KB size limitation. Be sure to account for variable length fields like firstName and lastName and ensure that, even when the maximum space is used in a field, that you are still below the 32KB limitation.

- **Clean-up** – If data persistence isn’t required, you can set an attribute with the same name and a blank value to prevent the data from being stored to the contact record or passed in a screen pop to an agent using the Amazon Connect Streams API while freeing up the bytes that data would have otherwise used in the contact record.

- **Sensitive data** – Use the Store customer input block to collect sensitive DTMF input from your contacts and use envelope encryption to protect both the raw data and the data keys used to encrypt them. Store sensitive data in a separate database where persistence is required, use the Set logging behavior flow block to disable logging whenever sensitive information is referenced, and remove, clean up, or obfuscate sensitive data using the Set contact attributes block Clean-up method outlined previously. For more information, see Compliance validation in Amazon Connect.
Telephony

In the US, use toll-free phone numbers wherever possible to load balance across multiple carriers for additional route and carrier redundancy. This also helps to decrease time to resolution when compared to DID phone numbers, which must be managed by a single carrier. In situations where you use DIDs, load balance across numbers from multiple carriers, when possible, to increase reliability. Make sure that you handle all error paths in your flow appropriately, and implement the best practices, requirements, and recommendations located in Troubleshooting Issues with the Contact Control Panel (CCP).

If you're forwarding your existing telephony provider's phone numbers to Amazon Connect, ensure that the process to change the forward destination to an alternative DID/toll-free number or otherwise remove the forward is defined and well-understood by your operations team. Ensure that you have Runbooks and Playbooks specifically for production readiness assessments, phone number porting and forwarding processes, and troubleshooting audio issues that could arise when transferring calls from your existing telephony provider. You also want a repeatable process that your operations team can follow to determine if the source of these audio issues is Amazon Connect or your existing telephony provider.

Amazon Connect APIs

Amazon Connect throttling quotas are by account, and not instance. You should consider the following best practices when working with Amazon Connect APIs:

Implement a caching/queuing solution

To decrease API data query overhead and avoid throttling, you can use an intermediary database like Amazon DynamoDB to store API call results rather than calling the API from all endpoints interested in the API data. For example, the following diagram represents the use of the Amazon Connect metric API from multiple sources that need to consume this information:
Rather than having separate AWS Lambda functions, each with their own polling requirements, you can have a single AWS Lambda function write all interesting data to Amazon DynamoDB. Rather than having each endpoint go to the API directly to retrieve the data, they point to DynamoDB, as illustrated in the following diagram:
This architecture allows you to change polling intervals and add endpoints, as needed, without worrying about exceeding service quotas, giving you the ability to scale to however many concurrent connections your database solution supports. You can use this same concept with querying any real-time data feeds from Amazon Connect. For situations where you need to perform an API action, like an Outbound API call, you can use this same concept in combination with Amazon Simple Queue Service to queue API requests Using AWS Lambda with SQS.

**Exponential back off and retry strategies**

You can run into situations where API throttling limits get exceeded. This can happen when the API calls fail and are retried repeatedly or made directly from multiple concurrent endpoints without a caching or queuing solution implemented. To avoid exceeding your service quotas and impacting downstream processes, you should consider using exponential back off and retry strategies within your AWS Lambda functions in combination with caching and queueing.
**Change management**

Two of the primary drivers for moving workloads to the Amazon Connect are flexibility and speed to market. To ensure operational excellence without sacrificing agility, follow these best practices:

- **Modular flows**: Flows in Amazon Connect are similar to modern application building where smaller, purpose-built components allow for more flexibility, control, and ease of management when compared to monolithic alternatives. You can make your flows small and re-usable, combining the modular flows into an end-to-end experience with Transfer to flow blocks. This approach allows you to reduce risk during change implementation, allow you to test single, smaller changes rather than regression testing the entire experience, and will make it easier to identify and address issues with your flows during testing.

- **Repositories**: Back up all versions of all flows to a repository of your choice using contact flow Import/Export as part of your change management process.

- **Distribute by percentage**: To reduce risk encountered during change management and experiment with new experiences for your contacts, you can use the Distribute by percentage block to route a subset of your traffic to new flows while leaving the other traffic on the original experience.

- **Measuring results**: Data driven decision making is key to successfully driving meaningful changes for your business. Having a key metric to measure your changes against is absolutely necessary. For all changes you're making, you need to plan for how you will measure success. For example, if you're implementing self-service functionality for your contacts, what percentage of contacts do you expect to self-serve to consider the workload successful or what other metrics are you measuring to determine success?

- **Rollbacks**: Ensure that there is a clear, well-defined, and well-understood process to back out any changes to the previous state, specific to the change performed. For example, if you publish a new flow version, ensure that the change instructions include documentation on how to roll back to the previous flow version.

**Routing profiles**

Understanding how priority, delay, and overflow routing work within Amazon Connect is critical to maximizing agent productivity, reducing contact wait times, and ensuring the best quality of experience for your contacts.
Routing in Amazon Connect

Contact routing in Amazon Connect is done through a collection of queues and routing configurations called a routing profile. A queue is equivalent to a skill or proficiency that an agent needs to possess to service contacts for that queue. A routing profile can be viewed as a set of skills that you can match to your contact’s needs.

Within your flow, you can prompt for additional information and, if they need to reach an agent, you can use the flow configuration to place them in the appropriate queue. In the following example, Savings, Checking, and Loans are individual queues or skills and the three routing profiles are unique skillsets, or groups of skills:

Each agent is assigned to only one routing profile based on their skillset, and many agents with similar skillset can share the same routing profile:
Each phone number or chat endpoint will be associated with one flow. The flow executes its logic, which may involve prompting the customer for information, to determine the contact’s needs, and eventually routes the contact into an appropriate queue. The following diagram depicts how routing profile, queue, and flow work together to service a contact:

To illustrate how you might determine various queues, routing profiles, and agent assignments to the routing profiles, consider the following table:

<table>
<thead>
<tr>
<th>Agent</th>
<th>Checking</th>
<th>Savings</th>
<th>Loans</th>
<th>Mortgages</th>
<th>Investments</th>
</tr>
</thead>
<tbody>
<tr>
<td>John D.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sam J.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debbie E.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Charles T.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jane D.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connie E.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Steve L.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chris A.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joyce C.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Brian M.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Caleb S.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Travis F.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Robbie H.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On the top row, you’ve identified your skills or queues. In the left column, you have your list of agents, and in the middle, you’ve checked the skills supported by each of the agents. You can sort the matrix grouped by the common set of skill requirements across our agent population. This helps identify the routing profiles as one marked in the green box (which consists of two queues), which you can assign agents to. As a result of this exercise, you have identified four routing profiles, and assign your 13 agents to them accordingly.

Based on the previous table, an incoming call from a contact needing the Savings skill could be served by three groups of agents in the three routing profiles 1, 2, and 4 as depicted in the following diagram:

![Diagram showing routing profiles](image)

**Priority and delay**

Using the combination of priority and delay in different Routing Profiles, you can create flexible routing strategies.
The preceding routing profile example shows a set of queues, and their respective priority and delay. The lower the number, the higher the priority. All higher priority calls must be processed before a lower priority call will be processed. This is a difference from systems that will eventually process lower priority of calls based upon a weighting factor.

You can also add a delay to each of the queues within each of the routing profiles. Any call coming into the queue will be held for the specified period of delay assigned to the designated queue. The call will be held for the delay period, even when agents are available. You might use this in situations where you have a group of agents who are reserved to help you meet your Service Level Agreements (SLAs), but are otherwise assigned to other tasks or queues. If a call doesn’t get answered within a specified period of time, these agents would become eligible to receive a call from the designated queue. For example, consider the following diagram:
This diagram shows an SLA of 30 seconds. A call comes in for the Savings queue. The Savings queue immediately looks for an agent in the "Savings" routing profile due to the configuration of 0 delay in the profile for the queue. Because of the configuration of 15 delay for Senior Agents, they will not be eligible to receive the Savings contact for 15 seconds. After 15 seconds elapses, the contact becomes available for a Senior Level agent and Amazon Connect looks for the Longest Available across both routing profiles.

Path to service

When you are designing customer experiences in Amazon Connect, plan to ensure a path to service. There are many planned and unplanned events that can impact the customer experience as they traverse through Amazon Connect Flows. The following sample customer experience shows some suggested checks to ensure a consistent quality experience for your contacts:
This sample customer experience takes into account planned events such as Holidays and Business hours as well as unplanned events, like agents not staffed during business hours. With this logic, you can also account for emergency situations, such as contact center closures because of inclement weather or service disruptions. Consider the following concepts as illustrated in the diagram:

- **Self-service**: In a typical IVR, you can include any greetings and disclaimer messages such as call recording announcements upfront, which can be followed by self-service options. Self-service brings cost and performance optimizations for your contact center and enables your organization to serve customers 24x7, regardless of holidays, business hours, or availability of agents. Always include a path to service in case customers are unable to self-serve and need human assistance. For example, if you are using Amazon Lex bots for self-service, you can make use of fallback intents to escalate conversations for human assistance.
• **Holidays**: Many enterprise customers have a central repository that holds corporate holidays. You can use an AWS Lambda function to data dip into that repository and offer holiday treatment to customers. Additionally, you can also store corporate holidays in DynamoDB along with a custom message for each holiday. For example, if your enterprise observes December 25 as Christmas, you could have a holiday prompt or Text to Speech, "We are currently closed for Christmas. Please call back on December 26 when our normal business hours will resume."

![Diagram of Amazon Connect, Lambda, and DynamoDB](image)

• **Business hours**: After holidays have been verified, you can check for business hours and, if outside of business hours, you can change the experience dynamically for your contacts. If the contact occurs during business hours, you can identify customer intent for calls and map to certain queues in your contact center, increasing the likelihood of getting to the correct agent, and decreasing the amount of time it takes your contact to reach service. It is highly recommended to map defaults as customers could be calling for a reason you haven’t accounted for yet or may respond in a way you don’t expect.

• **Emergency messages**: After you have identified customer intent for call, it is suggested to implement an emergency check treatment. In the event of an emergency situation that impacts your contact center, you can store an emergency True/False flag in an intermediary database like DynamoDB. To allow your supervisors and administrators to set this flag dynamically, with no code, you can build a separate IVR that authenticates your Amazon Connect administrators based upon ANI and PIN number verification for internal use only. In the event of emergency, your supervisors can call into that dedicated line from their phones and after authentication set the Emergency flag to true for scenarios such as contact center closure due to inclement weather or ISP outage at the physical location of contact center.

• **Emergency message API**: You can also consider building an AWS API gateway with AWS Lambda function at the back end to set the Emergency flag to true/false securely in the database. Your supervisors can securely access that API through web to toggle disaster mode or dynamically toggle it in response to an external event. In your Amazon Connect instance, every contact that comes in through the flow will use AWS Lambda to check for that emergency flag and, in case of disaster mode, you can dynamically make announcements and provide a customer with a path
to service. This will further ensure business continuity and mitigate the impact of situations like these from affecting your customers.

- **Check agent staffing**: Before transferring to the queue in your flow, you can check agent staffing to ensure that an agent is logged in to service the contact. For example, you may have an agent busy servicing another contact that might become available in the next five minutes, or you may not have anyone logged into the system at all. During these instances, you will prefer a different customer experience rather than making them wait in the queue for an agent to become available.

- **Route to service**: When you transfer the call to the queue, you can offer queued callbacks, queue overflows, or tiered routing using Amazon Connect routing profiles to offer a consistent, high-quality experience for your callers that meet your Service Level requirements.

**Resources**

**Documentation**

- [DevOps and AWS](#)
- [Amazon Connect Service API Documentation](#)

**Blog**

- [How to handle unexpected contact spikes with Amazon Connect](#)

**Video**

- [DevOps at Amazon](#)

**Security: Design principles for developing a secure contact center**

Security includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. This section provides an overview of design principles, best practices, and questions surrounding security for Amazon Connect workloads.
Amazon Connect Security Journey

After you’ve made the decision to move your workload to Amazon Connect, in addition to reviewing Security in Amazon Connect and Security Best Practices for Amazon Connect, follow these guidelines and steps to understand and implement your security requirements relative to the following core security areas:

Understanding the AWS Security Model

When you move computer systems and data to the cloud, security responsibilities become shared between you and AWS. AWS is responsible for securing the underlying infrastructure that supports the cloud, and you’re responsible for anything you put on the cloud or connect to the cloud.

AWS Shared Responsibility Model

Which AWS services you use will determine how much configuration work you have to perform as part of your security responsibilities. When you use Amazon Connect, the shared model reflects AWS and customer responsibilities at a high-level, as shown in the following diagram.
AWS Shared Responsibility Model for Amazon Connect

Compliance Foundations

Third-party auditors assess the security and compliance of Amazon Connect as part of multiple AWS compliance programs. These include SOC, PCI, HIPAA, C5 (Frankfurt), and HITRUST CSF.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Services Compliance Programs.

Region selection

Region selection to host the Amazon Connect instance depends on data sovereignty restrictions and where the contacts and agents are based. After that decision is made, review network requirements for Amazon Connect and ports and protocols that you need to allow. Additionally, to reduce the blast radius use the domain allow list or allowed IP address ranges for your Amazon Connect instance.

For more information, see Set up your network.
AWS services integration

We recommend reviewing each AWS service in your solution against the security requirements of your organization. See the following resources:

- Security in AWS Lambda
- Security and Compliance in DynamoDB
- Security in Amazon Lex

Data Security in Amazon Connect

During your security journey, your security teams may require a deeper understanding of how data is handled in Amazon Connect. See the following resources:

- Detailed network paths for Amazon Connect
- Infrastructure security in Amazon Connect
- Compliance validation in Amazon Connect

Workload diagram

Review your workload diagram and architect an optimum solution on AWS. This includes analyzing and deciding which additional AWS services should be included in your solution and any third-party and on-premises applications that need to be integrated.

AWS Identity and Access Management (IAM)

Types of Amazon Connect Personas

There are four types of Amazon Connect personas, based on the activities being performed.
1. **AWS administrator** – AWS administrators create or modify Amazon Connect resources and may also delegate administrative access to other principals by using the AWS Identity and Access Management (IAM) service. The scope of this persona is focused on creating and administering your Amazon Connect instance.

2. **Amazon Connect administrator** – Service administrators determine which Amazon Connect features and resources employees should access within the Amazon Connect admin website. The service administrator assigns security profiles to determine who can access the Amazon Connect admin website and what tasks they can perform. The scope of this persona is focused on creating and administering your Amazon Connect contact center.

3. **Amazon Connect agent** – Agents interact with Amazon Connect to perform their job duties. Service users may be contact center agents or supervisors.

4. **Amazon Connect Service contact** – The customer who interacts with your Amazon Connect contact center.
IAM Administrator Best Practices

IAM Administrative access should be limited to approved personnel within your organization. IAM administrators should also understand what IAM features are available to use with Amazon Connect. For IAM best practices, see Security best practices in IAM in the IAM User Guide. Also see Amazon Connect identity-based policy examples.

Amazon Connect Service Administrator Best Practices

Service administrators are responsible for managing Amazon Connect users, including adding users to Amazon Connect, giving them their credentials, and assigning the appropriate permissions so they can access the features needed to do their job. Administrators should start with a minimum set of permissions and grant additional permissions as necessary.

Security profiles help you manage who can access the Amazon Connect dashboard and Contact Control Panel, and who can perform specific tasks. Review the granular permissions granted within the default security profiles available natively. Custom security profiles can be set up to meet specific requirements. For example, a power agent who can take calls but also has access to reports. After this is finalized, users should be assigned to the correct security profiles.

Multi-Factor Authentication

For extra security, we recommend that you require multi-factor authentication (MFA) for all IAM users in your account. MFA can be set up through AWS IAM or your SAML 2.0 identity provider, or Radius server, if that's more applicable for your use case. After MFA is set up, a third text box becomes visible on the Amazon Connect login page to provide the second factor.

Identity Federation

In addition to storing users in Amazon Connect, you can enable single sign-on (SSO) to Amazon Connect by using identity federation. Federation is a recommended practice to allow for employee lifecycle events to be reflected in Amazon Connect when they are made in the source identity provider.

Access to Integrated Applications

Steps within your flows may need credentials to access information in external applications and systems. To provide credentials to access other AWS services in a secure way, use IAM roles. An IAM role is an entity that has its own set of permissions, but that isn't a user or group. Roles also don’t have their own permanent set of credentials and are automatically rotated.
Credentials such as API keys should be stored outside of your flow application code, where they can be retrieved programmatically. To accomplish this, you can use AWS Secrets Manager or an existing third-party solution. Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically.

**Detective controls**

Logging and monitoring are important for the availability, reliability and, performance of contact center. You should log relevant information from Amazon Connect Flows to Amazon CloudWatch and build alerts and notifications based on the same.

You should define log retention requirements and lifecycle policies early on, and plan to move log files to cost-efficient storage locations as soon as practical. Amazon Connect public APIs log to AWS CloudTrail. You should review and automate actions set up based on CloudTrail logs.

Amazon S3 is the best choice for long-term retention and archiving of log data, especially for organizations with compliance programs that require log data to be auditable in its native format. After log data is in an S3 bucket, define lifecycle rules to automatically enforce retention policies and move these objects to other, cost-effective storage classes, such as Amazon S3 Standard - Infrequent Access (Standard - IA) or Amazon S3 Glacier.

The AWS cloud provides flexible infrastructure and tools to support both sophisticated in cooperation with offerings and self-managed centralized-logging solutions. This includes solutions such as Amazon OpenSearch Service and Amazon CloudWatch Logs.

Fraud detection and prevention for incoming contacts can be implemented by customizing Amazon Connect Flows per the customer requirements. As an example, customers can check incoming contacts against previous contact activity in DynamoDB, and then take action, such as disconnecting a contact because they are a blocked contact.

**Infrastructure protection**

Although there is no infrastructure to manage in Amazon Connect, there could be scenarios where your Amazon Connect instance needs to interact with other components or applications deployed in infrastructure residing on-premises. Consequently, it is important to ensure that networking boundaries are considered under this assumption. Review and implement specific Amazon Connect infrastructure security considerations. Also, review contact center agent and supervisor desktops or VDI solutions for security considerations.
You can configure a Lambda function to connect to private subnets in a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud to create a private network for resources such as databases, cache instances, or internal services. Amazon Connect your function to the VPC to access private resources during execution.

**Data protection**

Customers should analyze the data traversing through and interacting with the contact center solution.

- Third party and external data
- On-premises data in hybrid Amazon Connect architectures

After analyzing the scope of the data, data classifications should be performed paying attention to identifying sensitive data. Amazon Connect conforms to the AWS shared responsibility model. Data protection in Amazon Connect includes best practices like using MFA and TLS and the use of other AWS services, including Amazon Macie.

Amazon Connect handles variety of data related to contact centers. This includes phone call media, call recordings, chat transcripts, contact metadata as well as flows, routing profiles and queues. Amazon Connect handles data at rest by segregating data by account ID and instance ID. All data exchanged with Amazon Connect is protected in transit between the user's web browser and Amazon Connect using open standard TLS encryption.

You can specify AWS KMS keys to be used for encryption including bring your own key (BYOK). Additionally, you can use key management options within Amazon S3.

**Protecting Data Using Client-Side Encryption**

Your use case may require encryption of sensitive data that is collected by flows. For example, to gather appropriate personal information to customize the customer experience when they interact with your IVR. To do this you can use public-key cryptography with the AWS Encryption SDK. The AWS Encryption SDK is a client-side encryption library designed to make it efficient for everyone to encrypt and decrypt data using open standards and best practices.

**Input validation**

Perform input validation to ensure that only properly formed data is entering the flow. This should happen as early as possible in the flow. For example, when prompting a customer to say or enter a telephone number, they may or may not include the country code.
Amazon Connect security vectors

Amazon Connect security can be divided into three logical layers as illustrated in the following diagram:

1. **Agent workstation.** The agent workstation layer is not managed by AWS and consists of any physical equipment and third-party technologies, services, and endpoints that facilitate your agent's voice, data, and access the Amazon Connect interface layer.

   Follow your security best practices for this layer with special attention to the following:
   - Plan identity management keeping in mind best practices noted in [Security Best Practices for Amazon Connect](#).
• Mitigate insider threat and compliance risk associated with workloads that handle sensitive information, by creating a secure IVR solution that enables you to bypass agent access to sensitive information. By encrypting contact input in your flows, you’re able to capture information securely without exposing it to your agents, their workstations, or their operating environments. For more information, see Encrypt customer input.

• You are responsible for maintaining the allowlist of AWS IP addresses, ports, and protocols needed to use Amazon Connect.

2. AWS: The AWS layer includes Amazon Connect and AWS integrations including AWS Lambda, Amazon DynamoDB, Amazon API Gateway, Amazon S3, and other services. Follow the security pillar guidelines for AWS services, with special attention to the following:


• Integrations with other AWS services: Identify each AWS service in the use case as well as any third-party integration points applicable for this use case.

• Amazon Connect can integrate with AWS Lambda functions that run inside of a customer VPC through the VPC endpoints for Lambda.

3. External: The External layer includes contact points including chat, click-to-call endpoints, and the PSTN for voice calls, integrations you may have with legacy contact center solutions in a Hybrid contact center architecture, and integrations you may have with other third-party solutions. Any entry point or exit point for a third party in your workload is considered the external layer.

This layer also covers integrations customers may have with other third-party solutions and applications such as CRM systems, work force management (WFM), and reporting and visualization tools and applications, such as Tableau and Kibana. You should consider the following areas when securing the external layer:

• You can create contact filters for repeat and fraudulent contacts using AWS Lambda to write contact details to DynamoDB from within your flow, including ANI, IP address for click-to-dial and chat endpoints, and any other identifying information to track how many contact requests occur during a given period of time. This approach allows you to query and add contacts to deny lists, automatically disconnecting them if they exceed reasonable levels.

• ANI Fraud detection solutions using Amazon Connect telephony metadata and partner solutions can be used to protect against caller ID spoofing.
• **Amazon Connect Voice ID** and other voice biometric partner solutions can be used to enhance and streamline the authentication process. Active voice biometric authentication allows contacts the option to speak specific phrases and use those for voice signature authentication. Passive voice biometrics allow contacts to register their unique voiceprint and use their voiceprint to authenticate with any voice input that meets sufficient length requirements for authentication.

• Maintain the **application integration** section in the Amazon Connect console for adding any third-party application or integration points to your allowlist, and remove unused endpoints.

• Send only the data necessary to meet minimum requirements to external systems that handle sensitive data. For example, if you have only one business unit using your call recording analytics solution, you can set an AWS Lambda trigger in your S3 bucket to process contact records, check for the business unit’s specific queues in the contact record data, and if it is a queue that belongs to the unit, send only that call recording to the external solution. With this approach, you only send the data necessary and avoid the cost and overhead associated with processing unnecessary recordings.

For an integration that enables Amazon Connect to communicate with Amazon Kinesis and Amazon Redshift to enable the streaming of contact records, see [Amazon Connect integration: Data streaming](#).

**Resources**

**Documentation**

• [AWS Cloud Security](#)
• [Security in Amazon Connect](#)
• [IAM Best Practices](#)
• [AWS Compliance](#)
• [AWS Security blog](#)

**Articles**

• [Security Pillar](#)
• [Introduction to AWS Security](#)
• [AWS Security Best Practices](#)
Videos

- AWS Security State of the Union
- AWS Compliance - The Shared Responsibility Model

Reliability

Reliability includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. As resiliency is handled as part of the service, there are no reliability practices unique to Amazon Connect beyond what is covered in Operational Excellence. You can find prescriptive guidance on implementation in the Reliability Pillar whitepaper.

Resources

Documentation

- AWS Service quotas
- Resilience in Amazon Connect
- Amazon CloudWatch

Whitepaper

- Reliability Pillar

Video

- Embracing Failure: Fault-Injection and Service Reliability

Product

- Trusted advisor: An online tool that provides you real-time guidance to help you provision your resources following AWS best practices.
Performance efficiency

Performance efficiency includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve. This section provides an overview of design principles, best practices, and questions surrounding performance efficiency for Amazon Connect workloads. You can find prescriptive guidance on implementation in the Performance Efficiency Pillar whitepaper.

Architectural design

There are two fundamental architectural design principles to consider when designing experiences for the contact center:

- Reductionism is a philosophical tenet stating that by analyzing a system to its ultimate component parts, you can unravel it at deeper levels.
- Holism, in contrast, states that by considering the whole picture one gets a deeper and more complete view of a situation than by analyzing it into its component parts.

The reductionist approach focuses on each individual component (IVR, ACD, Speech Recognition) on its own and often results in a disjointed customer experience that, when evaluated individually, may meet performance requirements for the use case. However, when evaluated end-to-end, can result in decreased quality of experience for your contacts while funneling development efforts into operational silos. This approach complicates regression testing, increases time to market, and limits the development of cross-discipline operational resources critical to the success of your contact center.

A holistic view of the contact center is shown in the following diagram:
The holistic approach results focus on a more complete and cohesive experience for customers, and not which technology will provide which part of that experience.

Let the customer and what they want define and guide your efforts. The experiences that you create for your contacts should not be static or an end state, but should serve as a starting point that should be iterated on continuously based on customer feedback. The regular collection and review of operational and tuning data surrounding how your contacts are interacting and navigating throughout their journey should drive that iteration. Your goal should be dynamic and personalized experiences for contacts reaching your company. This can be accomplished through dynamic data-driven contact design and routing, resulting in an experience that conforms to your contact and their individual needs.

You can start with the default experience, building out your flows, but refactoring your single flow into two to enable future segmentation:
In your next iteration, identify additional experiences that you need to plan for and build routing and, if necessary, flows for each. For example, you may want to play different prompts for a contact that is past due on their bill or that may have tried to contact multiple times for the same purpose. With this approach, you are working towards personalized, dynamic experiences that are pertinent to your contacts and why they are contacting you. In addition to improving the quality of experience for your contacts and decreasing handle times, you’re encouraging contact self-service by providing a more intelligent and flexible experience. Your next iteration may look like the following illustration:
Flow design

A flow defines the customer experience with your contact center from start to finish. Your flow configuration can have a direct impact on performance, operational efficiency, and ease of maintenance.

Many large businesses support multiple phone numbers, business units, prompts, queues, and other Amazon Connect resources. While it is possible to have unique flows for each phone number and line of business, it can lead to a one-to-one mapping of phone numbers and flows. This results in unnecessary service quota requests and a large number of flows to support and maintain. A one-to-one mapping of DNIS and Flow implementation is illustrated in the following figure:
Alternatively, you should consider an approach that results in Multiple DNIS to one or few flows by using the dynamic nature of Amazon Connect Flows. With this approach, you can store configuration information like Prompts, Queues, Business Hours, Whisper Prompts/Flows, Queues, Queue Treatments and Hold Messages etc., in NoSQL Database DynamoDB. In Amazon Connect, you can associate multiple phone numbers to the same flow and use the Lambda function to look up configurations for that phone number. This allows you to dynamically define the contact’s experience based on the attributes returned from DynamoDB.

For example, you can play prompts or use Text-to-Speech (TTS) to greet callers based upon the lookups in DynamoDB or associate queues using dynamic attributes supported in flow blocks. The result with this approach is a flow implementation that is efficient to build, maintain, and support:
Load testing

If you need to run load or scale testing, you can employ third-party or partner solutions to run load tests, or develop your own custom solution using the Amazon Connect StartOutboundVoiceContact API to generate calls combined with browser automation scripts to simulate agent behavior. Before performing load tests, review and follow the Amazon Connect Load Testing Policy.

Agent enablement

Amazon Connect provides a readily available browser-based Contact Control Panel (CCP) for agents to interact with customer contacts. Your agents use the CCP to accept contacts, chat with contacts, transfer them to other agents, put them on hold, and perform other key tasks. You can realize significant performance efficiency through the creation of custom agent desktop solutions using the Amazon Connect Streams API. Consider using the Streams API to increase performance efficiency in the following areas:

- CRM integration - The Streams API allows you to embed the CCP in your CRM application, create your own interface, or integrate with other AWS services and partner solutions to provide your agents with the tools and resources they need to service your contacts. With a custom desktop, like the Amazon Connect and Salesforce integration, your agents can get a comprehensive view of customer and contact in a single interface without managing multiple screens and interfaces.
• Authentication - You can configure SAML for identity management in Amazon Connect and use IAM Identity Center (SSO) to allow your agents to use the same credentials they use to access your other systems and avoid the need to enter them multiple times.

• Agent automation - In addition to streamlining your agent experience, you can automate common, repeatable tasks. For example, automatically creating cases or pre-filling webforms and offering a screen pop with relevant information when a contact is offered. This can reduce handle times and improve the quality of experience for your agents and contacts.

• Enhanced capabilities - You can also enhance/extend the CCP functionality to include real-time Transcriptions, Translations, Suggested Actions and Knowledge base integrations. Integrating enhanced capabilities with your agent desktop will allow skilled agents to service contacts more efficiently and unskilled agents to provide service when skilled agents aren’t available. For example, you can use this approach to automatically translate a chat contact for unskilled agent that doesn’t know the language. When your agent replies, you can automatically translate the text to the contact’s language, allowing for real-time bilingual communication.

Using other AWS services

This section discusses AWS services that you can use to improve performance, identify areas of opportunity, and gain valuable insights into your contact data.

AWS Lambda

You can use AWS Lambda in your Amazon Connect Flows to perform data dips for customer information, send SMS text messages, and with other services like Amazon S3 to automatically distribute scheduled reports. For more information, see Best Practices for Working with AWS Lambda functions.

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it more efficient to establish a dedicated network connection from your premises to AWS. It provides a durable, consistent connection rather than relying on your ISP to dynamically route requests to AWS resources. It allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN and establish private connectivity between AWS and your data center, office, or colocation environment. In many cases, this can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
While AWS Direct Connect does not solve issues specific to private LAN/WAN traversal to your edge router, it can help solve for latency and connectivity issues between your edge router and AWS resources. It can also solve for latency and poor call quality between your edge router and AWS resources.

Depending on your VDI environment, you may not be able to take advantage of AWS Direct Connect as it requires you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN. If the VDI environment is hosted outside of your local DXC-enabled network, you may not be able to take full advantage of AWS Direct Connect.

Do not use AWS Direct Connect for "QoS" or "increased security." AWS Direct Connect can cause performance degradation in cases where the latency from the agent workstation is higher than the ISP's path to the Amazon Connect instance. AWS Direct Connect does not offer additional security when compared to an ISP as Amazon Connect voice and data is already encrypted.

**Amazon Polly**

Amazon Connect offers a native integration with Amazon Polly, allowing you to play dynamic and natural Text-to-Speech (TTS), use Speech Synthesis Markup Language (SSML), and take advantage of Neural Text-to-Speech (NTTS) to achieve the most natural and human-like text-to-speech voices possible.

**Amazon Lex**

Your contact's path to service can be a challenging experience that doesn't always meet up to their expectations. Your contacts may wait on hold, repeat information, need to be transferred, and ultimately, spend too much time getting what they need. AI is playing a role in improving this customer experience in call centers to include engagement through chatbots — intelligent, natural language virtual assistants. These chatbots are able to recognize human speech and understand the caller's intent without requiring the caller to speak in specific phrases. Contacts can perform tasks such as changing a password, requesting a balance on an account, or scheduling an appointment without ever speaking to an agent.

Amazon Lex is a service that allows you to create intelligent conversational chatbots. It lets you turn your Amazon Connect contact center flows into natural conversations that provide personalized experiences for your callers. Using the same technology that powers Amazon Alexa, an Amazon Lex chatbot can be attached to your Amazon Connect Flow to recognize the intent of your caller, ask follow-up questions, and provide answers. Amazon Lex maintains context and manages the dialogue, dynamically adjusting the responses based on the conversation, so your
contact center can perform common tasks for callers, to address many customer inquiries through self-service interactions. Additionally, Amazon Lex chatbots support an optimal (8 kHz) telephony audio sampling rate, to provide increased speech recognition accuracy and fidelity for your contact center voice interactions.

Building an effective Amazon Lex bot requires providing simple and realistic utterances as training sets to the bot, periodically reviewing your bot’s performance, updating your utterance set, and modifying the bot based on such a review. For more information, see the following resources:

- [Monitoring in Amazon Lex](#)
- [Building Better bots using Amazon Lex](#)

Amazon Kinesis

For situations where you need to gain additional insight from your contact metrics and real-time data from Amazon Connect, you can:

- Export your contact record data to Amazon Redshift using Amazon Kinesis.
- Use Amazon Kinesis video stream (KVS) and AWS Lambda to transcribe call recordings or voice contacts in real-time using Amazon Transcribe and send the resulting text to Amazon Comprehend for sentiment analysis.
- Leverage the [Amazon Connect Agent Event Kinesis Stream](#) for real-time agent CTI and schedule adherence data.

Amazon OpenSearch Service and Kibana

Using Amazon OpenSearch Service and Kibana to process real-time Amazon Connect data gives you a flexible way to query and visualize real-time and historical Amazon Connect data beyond native reporting capabilities.

Amazon Connect Contact Lens

Contact Lens for Amazon Connect is a set of machine learning (ML) capabilities integrated into Amazon Connect that allow contact center supervisors to better understand the sentiment, trends, and compliance risks of customer conversations to effectively train agents, replicate successful interactions, and identify crucial company and product feedback. Contact Lens for Amazon Connect transcribes contact center calls to create a fully searchable archive and surface valuable customer insights.
Cost optimization

Cost Optimization includes the ability to run systems to deliver business value at the lowest price point. This section provides an overview of design principles, best practices, and questions surrounding cost optimization for Amazon Connect workloads. You can find prescriptive guidance on implementation in the Cost Optimization Pillar whitepaper.

There are five areas to consider for cost optimization for Amazon Connect workloads.

Region selection

Amazon Connect Region selection is one of the first decision customers make when adopting Amazon Connect for their contact center workloads. While latency and voice quality are important aspects to Region selection, you should evaluate Region selection from a cost perspective as well. Telephony pricing for Claimed Phone Numbers Per Day and Per Minute Inbound Usage can be different for countries depending upon the AWS Region in which you select to instantiate your Amazon Connect Instance. You can find telephony price for each Region at Amazon Connect Pricing page.

Callbacks

You can provide a callback in your flow for callers during high call volume periods or long wait times. You can use callbacks to reduce cost and improve the quality of experience for your contacts.
When your contact opts-in for the callback, Amazon Connect will retain the position in the queue and allow the caller to disconnect. When an agent becomes available to service your contact, Amazon Connect will place an outbound call to the number configured to connect the contact to your agent. A sample callback flow is included in every instance at creation. You can also use AWS Lambda and Amazon DynamoDB to prevent duplicate callback requests.

Storage

With Amazon Connect, you can configure your instance and flows to store call recordings and chat transcripts of caller’s interactions for compliance, quality monitoring, and training purposes. Voice contacts are not recorded unless an agent is connected to the caller. If multiple agents are connected, each will have an associated call recording or transcript. Amazon Connect stores voice recordings in Amazon S3 according to your Amazon S3 Lifecycle policy configuration. With the call recordings stored in Amazon S3, you can use Amazon S3 tiers of storage to manage retention and optimize cost. For example, you can transition objects using Amazon S3 Lifecycle to move call recordings and transcripts over three months old to S3 Glacier to reduce storage cost.

Self-service

Amazon Connect’s pay-as-you-go pricing model can result in lower costs as compared to traditional licensing-based contact centers. However, the traditional contact center infrastructure that spans automatic call distribution (ACD) systems, IVR, telephony and work force management (WFM) systems plays a proportionately small contribution to the overall cost of contact center operations. The largest contributor to the cost of the contact center often comes from human capital and the real estate required to provide an operating environment for your agents. Amazon Connect Flows can be used natively with Amazon Lex for NLU, NLP, and ASR and Amazon Polly for lifelike Text-to-Speech (TTS) to build highly engaging user experiences and natural conversational interactions across voice and text. By using an Amazon Lex chatbot in your Amazon Connect call center, callers can perform tasks such as changing a password, requesting a balance on an account, or scheduling an appointment, without needing to speak to an agent. These self-service options result in better customer experience and lowers your cost per contact.
Click-to-call

You can use click-to-call in Amazon Connect to initiate a voice call using the `StartOutboundVoiceContact` API for authentication through web or mobile application to reduce call handle times and improve the quality of experience. With this approach, you’re able to offer your contact the ability to bypass IVR authentication, pass contextual information like URLs, recent web/mobile activity, and user data to your flows to create dynamic, personalized experiences. For example, a contact browsing your website to purchase an item or member of a financial institution who is already authenticated in the mobile app and wants to speak with an agent about a recent transaction.

Redirect voice contacts to chat

With Amazon Connect, you can allow agents to handle multiple chat conversations simultaneously where they would only able to handle one voice conversation. When you don't have a voice agent available, you can send an SMS text message to your customer to offer a link to chat with an agent right away.

Resources

Documentation
Plan your identity management in Amazon Connect

Before you set up your Amazon Connect instance, you should decide how you want to manage your Amazon Connect users. A user is anyone who needs an Amazon Connect account: agents, call center managers, analysts, and more.

You cannot change the option you select for identity management after you create an instance. Instead, you must delete the instance and create a new one. However, if you delete an instance, you lose its configuration settings and metrics data.

When you create your instance, you can choose from one of the following identity management solutions:

- **Store users with Amazon Connect**—Choose this option if you want to create and manage user accounts within Amazon Connect.

  When you manage users in Amazon Connect, the user name and password for each user is specific to Amazon Connect. Users must remember a separate user name and password to log in to Amazon Connect.

- **Link to an existing directory**—Choose this option to use an existing Active Directory. Users will log in to Amazon Connect using their corporate credentials.

  If you choose this option, the directory must be associated with your account, set up in AWS Directory Service, and be active in the same Region in which you create your instance. If you plan to choose this option, you should prepare your directory before you create your Amazon Connect instance. For more information, see **Use an existing directory for identity management**.

- **SAML 2.0-based authentication**—Choose this option if you want to use your existing network identity provider to federate users with Amazon Connect. Users can only log in to Amazon Connect by using the link configured through your identity provider. If you plan to choose
this option, you should configure your environment for SAML before you create your Amazon Connect instance. For more information, see Configure SAML with IAM for Amazon Connect.

Use an existing directory for identity management

If you are already using a AWS Directory Service directory to manage users, you can use the same directory to manage user accounts in Amazon Connect. You can also create a new directory in AWS Directory Service to use for Amazon Connect. The directory you choose must be associated with your AWS account, and must be active in the AWS Region in which you create your instance. You can associate an AWS Directory Service directory with only one Amazon Connect instance at a time. To use the directory with a different instance, you must delete the instance with which it is already associated.

The following AWS Directory Service directories are supported in Amazon Connect:

- **Microsoft Active Directory**—AWS Directory Service lets you run Microsoft Active Directory as a managed service.
- **Active Directory Connector**—AD Connector is a directory gateway you can use to redirect directory requests to your on-premises Microsoft Active Directory.
- **Simple Active Directory**—Simple AD is a standalone managed directory that is powered by a Samba 4 Active Directory compatible server.

You cannot change the identity option you select after you create the instance. If you decide to change the directory you selected, you can delete the instance and create a new one. When you delete an instance, you lose all configuration settings and metrics data for it.

There is no additional charge for using an existing or a proprietary directory in Amazon Connect. For information about the costs associated with using AWS Directory Service, see AWS Directory Service Pricing Overview.

The following limitations apply to all new directories created using AWS Directory Service:

- Directories can only have alphanumeric names. Only the '.' character can be used.
- Directories cannot be unbound from an Amazon Connect instance after they have been associated.
- Only one directory can be added to an Amazon Connect instance.
- Directories cannot be shared across multiple Amazon Connect instances.
Configure SAML with IAM for Amazon Connect

Amazon Connect supports identity federation by configuring Security Assertion Markup Language (SAML) 2.0 with AWS IAM to enable web-based single sign-on (SSO) from your organization to your Amazon Connect instance. This allows your users to sign in to a portal in your organization hosted by a SAML 2.0 compatible identity provider (IdP) and log in to an Amazon Connect instance with a single sign-on experience without having to provide separate credentials for Amazon Connect.

Important notes

Before you begin, note the following:

- These instructions do not apply to Amazon Connect Global Resiliency deployments. For information that applies to Amazon Connect Global Resiliency, see [Integrate your identity provider (IdP) with a new AWS sign in SAML endpoint](#).
- Choosing SAML 2.0-based authentication as the identity management method for your Amazon Connect instance requires the configuration of [AWS Identity and Access Management federation](#).
- The user name in Amazon Connect must match the RoleSessionName SAML attribute specified in the SAML response returned by the identity provider.
- Amazon Connect does not support reverse federation. That is, you can't login directly into Amazon Connect. If you tried, you'd get a `Session Expired` message. The authentication should be done from the Identity Provider (IdP) and not the Service Provider (SP) (Amazon Connect).
- Most identity providers by default use the global AWS sign-in endpoint as the Application Consumer Service (ACS), which is hosted in US East (N. Virginia). We recommend overriding this value to use the regional endpoint that matches the AWS Region where your instance was created.
- All Amazon Connect usernames are case sensitive, even when using SAML.
- If you have old Amazon Connect instances that were set up with SAML and you need to update your Amazon Connect domain, see [Personal settings](#).

Overview of using SAML with Amazon Connect

The following diagram shows the flow for SAML requests to authenticate users and federate with Amazon Connect.
SAML requests go through the following steps:

1. The user browses to an internal portal that includes a link to log in to Amazon Connect. The link is defined in the identity provider.

2. The federation service requests authentication from the organization's identity store.

3. The identity store authenticates the user and returns the authentication response to the federation service.

4. When authentication is successful, the federation service posts the SAML assertion to the user's browser.

5. The user's browser posts the SAML assertion to the AWS sign in SAML endpoint (https://signin.aws.amazon.com/saml). AWS sign in receives the SAML request, processes the request, authenticates the user, and forwards the authentication token to Amazon Connect.

6. Using the authentication token from AWS, Amazon Connect authorizes the user and opens Amazon Connect in their browser.
Enabling SAML-based authentication for Amazon Connect

The following steps are required to enable and configure SAML authentication for use with your Amazon Connect instance:

1. Create an Amazon Connect instance and select SAML 2.0-based authentication for identity management.
2. Enable SAML federation between your identity provider and AWS.
3. Add Amazon Connect users to your Amazon Connect instance. Log in to your instance using the administrator account created when you created your instance. Go to the User Management page and add users.

⚠️ Important

- Only the following special characters are allowed in the username: @ - .
- Due to the association of an Amazon Connect user and an AWS IAM Role, the user name must match exactly the RoleSessionName as configured with your AWS IAM federation integration, which typically ends up being the user name in your directory. The format of the username should match the intersection of the format conditions of the RoleSessionName and an Amazon Connect user, as shown in the following diagram:

Use the following format for user names:

- String: Upper- and lower-case alphanumeric characters with no spaces
- Length constraints: Minimum length of 2. Maximum length of 64.
- Special characters: @ - .
4. Configure your identity provider for the SAML assertions, authentication response, and relay state. Users log in to your identity provider. When successful, they are redirected to your Amazon Connect instance. The IAM role is used to federate with AWS, which allows access to Amazon Connect.

**Select SAML 2.0-based authentication during instance creation**

When you are creating your Amazon Connect instance, select the SAML 2.0-based authentication option for identity management. On the second step, when you create the administrator for the instance, the user name that you specify must exactly match a user name in your existing network directory. There is no option to specify a password for the administrator because passwords are managed through your existing directory. The administrator is created in Amazon Connect and assigned the **Admin** security profile.

You can log in to your Amazon Connect instance, through your IdP, using the administrator account to add additional users.

**Enable SAML federation between your identity provider and AWS**

To enable SAML-based authentication for Amazon Connect, you must create an identity provider in the IAM console. For more information, see [Enabling SAML 2.0 Federated Users to Access the AWS Management Console](#).

The process to create an identity provider for AWS is the same for Amazon Connect. Step 6 in the above flow diagram shows the client is sent to your Amazon Connect instance instead of the AWS Management Console.

The steps necessary to enable SAML federation with AWS include:

1. Create a SAML provider in AWS. For more information, see [Creating SAML Identity Providers](#).
2. Create an IAM role for SAML 2.0 federation with the AWS Management Console. Create only one role for federation (only one role is needed and used for federation). The IAM role determines which permissions the users that log in through your identity provider have in AWS. In this case, the permissions are for accessing Amazon Connect. You can control the permissions to features of Amazon Connect by using security profiles in Amazon Connect. For more information, see [Creating a Role for SAML 2.0 Federation (Console)](#).

   In step 5, choose **Allow programmatic and AWS Management Console access**. Create the trust policy described in the topic in the procedure **To prepare to create a role for SAML 2.0 federation**.
Then create a policy to assign permissions to your Amazon Connect instance. Permissions start on step 9 of the To create a role for SAML-based federation procedure.

To create a policy for assigning permissions to the IAM role for SAML federation

1. On the Attach permissions policy page, choose Create policy.
2. On the Create policy page, choose JSON.
3. Copy one of the following example policies and paste it into the JSON policy editor, replacing any existing text. You can use either policy to enable SAML federation, or customize them for your specific requirements.

Use this policy to enable federation for all users in a specific Amazon Connect instance. For SAML-based authentication, replace the value for the Resource to the ARN for the instance that you created:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement1",
         "Effect": "Allow",
         "Action": "connect:GetFederationToken",
         "Resource": [
            "arn:aws:connect:us-east-1:361814831152:instance/2fb42df9-78a2-2e74-d572-c8af67ed289b/user/${aws:userid}"
         ]
      }
   ]
}
```

Use this policy to enable federation to a specific Amazon Connect instances. Replace the value for the connect:InstanceId to the instance ID for your instance.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement2",
         "Effect": "Allow",
         "Action": "connect:GetFederationToken",
         "Resource": [
            "arn:aws:connect:us-east-1:361814831152:instance/2fb42df9-78a2-2e74-d572-c8af67ed289b/user/${aws:userid}"
         ]
      }
   ]
}
```
Use this policy to enable federation for multiple instances. Note the brackets around the listed instance IDs.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "connect:InstanceId": [
                        "2fb42df9-78a2-2e74-d572-c8af67ed289b",
                        "1234567-78a2-2e74-d572-c8af67ed289b"
                    ]
                }
            }
        }
    ]
}
```

4. After you create the policy, choose **Next: Review**. Then return to step 10 in the *To create a role for SAML-based federation* procedure in the [Creating a Role for SAML 2.0 Federation (Console)](https://aws.amazon.com/documentation/ses/index.html) topic.

3. Configure your network as a SAML provider for AWS. For more information, see [Enabling SAML 2.0 Federated Users to Access the AWS Management Console](https://aws.amazon.com/documentation/ses/index.html).

4. Configure SAML Assertions for the Authentication Response. For more information, see [Configuring SAML Assertions for the Authentication Response](https://aws.amazon.com/documentation/ses/index.html).

5. For Amazon Connect, leave the **Application Start URL** blank.
6. Override the Application Consumer Service (ACS) URL in your identity provider to use the regional endpoint that coincides with the AWS Region of your Amazon Connect instance. For more information, see Configure the identity provider to use regional SAML endpoints.

7. Configure the relay state of your identity provider to point to your Amazon Connect instance. The URL to use for the relay state is comprised as follows:

```
hitps://region-id.console.aws.amazon.com/connect/federate/instance-id
```

Replace the `region-id` with the Region name where you created your Amazon Connect instance, such as us-east-1 for US East (N. Virginia). Replace the `instance-id` with the instance ID for your instance.

For a GovCloud instance, the URL is `https://console.amazonaws-us-gov.com/`:

- `https://console.amazonaws-us-gov.com/connect/federate/instance-id`

**Note**

You can find the instance ID for your instance by choosing the instance alias in the Amazon Connect console. The instance ID is the set of numbers and letters after '/' instance' in the Instance ARN displayed on the Overview page. For example, the instance ID in the following instance ARN is `178c75e4-b3de-4839-a6aa-e321ab3f3770`.

```
arn:aws:connect:us-east-1:450725743157:instance/178c75e4-b3de-4839-a6aa-e321ab3f3770
```

### Configure the identity provider to use regional SAML endpoints

To provide the best availability we recommend using the regional SAML endpoint that coincides with your Amazon Connect instance instead of the default global endpoint.

The following steps are IdP agnostic; they work for any SAML IdP (for example, Okta, Ping, OneLogin, Shibboleth, ADFS, AzureAD, and more).

1. Update (or override) the Assertion Consumer Service (ACS) URL. There are two ways you can do this:
   
   - **Option 1**: Download the AWS SAML metadata and update the Location attribute to the Region of your choice. Load this new version of the AWS SAML metadata into your IdP.
Following is an example of a revision:

```xml
<AssertionConsumerService index="1" isDefault="true"
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://region-id.signin.aws.amazon.com/saml"/>
```

- **Option 2**: Override the AssertionConsumerService (ACS) URL in your IdP. For IdPs like Okta that provide prebaked AWS integrations, you can override the ACS URL in the AWS admin console. Use the same format to override to a Region of your choice (for example, https://region-id.signin.aws.amazon.com/saml).

2. Update the associated role trust policy:
   a. This step needs to be done for every role in every account that trusts the given identity provider.
   b. Edit the trust relationship, and replace the singular SAML:aud condition with a multivalued condition. For example:
          "https://region-id.signin.aws.amazon.com/saml" ]
   c. Make these changes to the trust relationships in advance. They should not be done as part of a plan during an incident.

3. Configure a relay state for the Region-specific console page.
   a. If you don't do this final step, there's no guarantee that the Region-specific SAML sign in process will forward the user to the console sign in page within the same Region. This step is most varied per identity provider, but there are a blogs (for example, How to Use SAML to Automatically Direct Federated Users to a Specific AWS Management Console Page) that show the use of relay state to achieve deep linking.
   b. Using the technique/parameters appropriate for your IdP, set the relay state to the console endpoint that matches (for example, https://region-id.console.aws.amazon.com/connect/federate/instance-id).

**Note**
- Ensure that STS is not disabled in your additional Regions.
Use a destination in your relay state URL

When you configure the relay state for your identity provider, you can use the destination argument in the URL to navigate users to a specific page in your Amazon Connect instance. For example, use a link to open the CCP directly when an agent logs in. The user must be assigned a security profile that grants access to that page in the instance. For example, to send agents to the CCP, use a URL similar to the following for the relay state. You must use URL encoding for the destination value used in the URL:


Another example of a valid URL is:


For a GovCloud instance, the URL is https://console.amazonaws-us-gov.com/. So the address would be:


If you want to configure the destination argument to a URL outside of the Amazon Connect instance, such as your own custom website, first add that external domain to the account's approved origins. For example, perform the steps in the following order:

1. In the Amazon Connect console add https://your-custom-website.com to your approved origins. For instructions, see Use an allowlist for integrated applications.

2. In your identity provider configure your relay state to https://your-region.console.aws.amazon.com/connect/federate/instance-id?
   destination=https%3A%2F%2Fyour-custom-website.com

3. When your agents log in they are taken directly to https://your-custom-website.com.
Add users to your Amazon Connect instance

Add users to your connect instance, making sure that the user names exactly match the users names in your existing directory. If the names do not match, users can log in to the identity provider, but not to Amazon Connect because no user account with that user name exists in Amazon Connect. You can add users manually on the User management page, or you can bulk upload users with the CSV template. After you add the users to Amazon Connect, you can assign security profiles and other user settings.

When a user logs in to the identity provider, but no account with the same user name is found in Amazon Connect, the following Access denied message is displayed.

Bulk upload users with the template

You can import your users by adding them to a CSV file. You can then import the CSV file to your instance, which adds all users in the file. If you add users by uploading a CSV file, make sure that you use the template for SAML users. You can find on the User management page in Amazon Connect. A different template is used for SAML-based authentication. If you previously downloaded the template, you should download the version available on the User management page after you set up your instance with SAML-based authentication. The template should not include a column for email or password.

SAML user logging in and session duration

When you use SAML in Amazon Connect, users must log in to Amazon Connect through your identity provider (IdP). Your IdP is configured to integrate with AWS. After authentication, a token for their session is created. The user is then redirected to your Amazon Connect instance and automatically logged in to Amazon Connect using single sign-on.

As a best practice, you should also define a process for your Amazon Connect users to log out when they are finished using Amazon Connect. They should log out from both Amazon Connect and your
identity provider. If they do not, the next person that logs in to the same computer can log in to Amazon Connect without a password since the token for the previous sessions is still valid for the duration of the session. It's valid for 12 hours.

**About session expiration**

Amazon Connect sessions expire 12 hours after a user logs in. After 12 hours, users are automatically logged out, even if they are currently on a call. If your agents stay logged in for more than 12 hours, they need to refresh the session token before it expires. To create a new session, agents need to log out of Amazon Connect and your IdP and then log in again. This resets the session timer set on the token so that agents are not logged out during an active contact with a customer. When a session expires while a user is logged in, the following message is displayed. To use Amazon Connect again, the user needs to log in to your identity provider.

![Session expired]

Your session has expired. Please log in again to continue. Sessions expire after 12 hours.

**Troubleshoot SAML with Amazon Connect**

This article explains how to troubleshoot and resolve some of the most common issues customers encounter when using SAML with Amazon Connect.

If you're troubleshooting your integration with other identity providers such as Okta, PingIdentify, Azure AD, and more, see [Amazon Connect SSO Setup Workshop](#).

**Error Message: Access Denied. Your account has been authenticated, but has not been onboarded to this application.**

![Access denied]

Your account has been authenticated, but has not been onboarded to this application. Contact your Administrator to onboard to Amazon Connect and try again.
What does this mean?

This error means that the user has successfully authenticated using SAML into the AWS SAML login endpoint. However, the user could not be matched/found inside Amazon Connect. This usually indicates one of the following:

- The username in Amazon Connect doesn't match the RoleSessionName SAML attribute specified in the SAML response returned by the identity provider.
- The user doesn't exist in Amazon Connect.
- The user has two separate profiles assigned to them with SSO.

Resolution

Use the following steps to check the RoleSessionName SAML attribute specified in the SAML response returned by the identity provider, and then retrieve and compare with the login name in Amazon Connect.

1. Perform a HAR capture (HTTP ARchive) for the end-to-end login process. This captures the network requests from the browser side. Save the HAR file with your preferred file name, for example, saml.har.

   For instructions, see How do I create a HAR file from my browser for an AWS Support case?

2. Use a text editor to find the SAMLResponse in the HAR file. Or, run the following commands:

   ```bash
   $ grep -o "SAMLResponse=.*&" azuresaml.har | sed -E 's/SAMLResponse=(.*)&/\1/' > samlresponse.txt
   
   • This searches for the SAMLResponse in the HAR file and saves it to a samlresponse.txt file.
   • The response is URL encoded and the contents are Base64 encoded.
   
   3. Decode the URL response and then decode the Base64 contents using a third-party tool or a simple script. For example:

   ```bash
   $ cat samlresponse.txt | python3 -c "import sys; from urllib.parse import unquote; print(unquote(sys.stdin.read()));" | base64 --decode > samlrespondedecoded.txt
   ```
This script uses a simple python command to decode the SAMLResponse from its original URL encoded format. Then it decodes the response from Base64 and outputs the SAML Response in plain text format.

4. Check the decoded response for the needed attribute. For example, the following image shows how to check RoleSessionName:

```bash
$ export username='grep -Eo 'RoleSessionName.*?'<AttributeValue>'

samldecoded.txt | sed 's/.*<AttributeValue>(.*)</AttributeValue>/1/'
```

5. Check whether the username returned in from the previous step exists as a user in your Amazon Connect instance:

```bash
$ aws connect list-users --instance-id [INSTANCE_ID] | grep $username
```

- If the final grep does not return a result then this means that the user does not exist in your Amazon Connect instance or it has been created with a different case/capitalization.
- If your Amazon Connect instance has many users, the response from the ListUsers API call maybe paginated. Use the NextToken returned by the API to fetch the rest of the users. For more information, see `ListUsers`.

**Example SAML Response**

Following is an image from a sample SAML Response. In this case, the identity provider (IdP) is Azure Active Directory (Azure AD).

```xml
<Attribute>
    <AttributeValue>jane-doe@examplecorp.com</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>https://aws.amazon.com/SAML/Attributes/Role</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>arn:aws:saml:1111111111:role/AzureAD_Role,arn:aws:saml:1111111111:provider/AzureAD\nConnect_Admns</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>https://aws.amazon.com/SAML/Attributes/RoleSessionName</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>amzn0-arn:1111111111:iam:access-key</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>AccessKeyId</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>https://aws.amazon.com/SAML/Attributes/SessionDuration</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>2020-03-17T08:31:42.838Z</AttributeValue>
</Attribute>
<Attribute>
    <AttributeValue>SessionIndex</AttributeValue>
</Attribute>
```

This is the returned RoleSessionName.
Error Message: Access denied, Please contact your AWS account administrator for assistance.

What does this mean?

The role that the user has assumed has successfully authenticated using SAML. However, the role doesn't have permission to call the GetFederationToken API for Amazon Connect. This call is required so the user can log in to your Amazon Connect instance using SAML.

Resolution

1. Attach a policy that has the permissions for connect:GetFederationToken to the role found in the error message. Following is a sample policy:

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [{
   "Sid": "Statement1",
   "Effect": "Allow",
   "Action": "connect:GetFederationToken",
   "Resource": [
   ]
   }]
   }
   ```

2. Use the IAM console to attach the policy. Or, use the attach-role-policy API, for example:

   ```bash
   $ aws iam attach-role-policy --role-name [ASSUMED_ROLE] --policy_arn [POLICY_WITH_GETFEDERATIONTOKEN]
   ```
Additional resources for Amazon Connect

In addition to using the contents of this guide, you can learn more about Amazon Connect by using the following resources.

Resources

- Amazon Connect API Reference
- Amazon Connect Participant Service API Reference
- Amazon AppIntegrations Service API Reference
- Contact Lens for Amazon Connect API Reference
- Amazon Connect Customer Profiles API
- Amazon Connect Voice ID API Reference
- Amazon Q in Connect API Reference
- Amazon Connect Streams
- Amazon Connect Chat UI Examples

Amazon Connect API Reference

The Amazon Connect API Reference describes the API actions that are used to set up and manage your contact center.

Amazon Connect Participant Service API Reference

The Amazon Connect Participant Service API Reference describes the API actions that are used to manage chat participants, such as agents and customers.

Amazon AppIntegrations Service API Reference

The Amazon AppIntegrations Service API Reference describes the API actions that you can use to configure connections to external applications.

Contact Lens for Amazon Connect API Reference

The Amazon Connect Contact Lens API Reference describes the API actions that you can use to access an up-to-date transcript, along with all the associated conversation characteristics while a
call is still in progress. This helps to reduce the need for agents to write detailed call summaries and enables a seamless handoff from one agent to another during a call transfer.

**Amazon Connect Customer Profiles API**

The [Amazon Connect Customer Profiles API Reference](#) describes the API actions that you can use to manage domains and profiles.

**Amazon Connect Voice ID API Reference**

The [Amazon Connect Voice ID API Reference](#) describes the API actions that provide real-time caller authentication and fraud screening.

**Amazon Q in Connect API Reference**

The [Amazon Q in Connect API Reference](#) describes the API actions that deliver information to agents to help them solve customer issues.

**Amazon Connect Streams**

The [Amazon Connect Streams](#) documentation describes how to integrate your existing web applications with Amazon Connect. Streams gives you the power to embed the Contact Control Panel (CCP) UI components into your page, and/or handle agent and contact state events directly giving you the power to control agent and contact state through an object oriented event driven interface. You can use the built in interface or build your own from scratch: Streams gives you the power to choose.

**Amazon Connect Chat UI Examples**

The [Amazon Connect Chat SDK and Sample Implementations](#) provides examples of how to enable your app to engage with Amazon Connect chat.

**Get administrative support for Amazon Connect**

If you are an administrator and need to contact support for Amazon Connect, choose one of the following options:

- If you have an AWS Support account, go to [Support Center](#) and submit a ticket.
• Otherwise, open the AWS Management Console and choose Amazon Connect, Support, Create case.

It's helpful to provide the following information:

• Your contact center instance ID/ARN. To find your instance ARN, see Find your Amazon Connect instance ID/ARN.
• Your region.
• A detailed description of the issue.
Set up your contact center

Amazon Connect enables you to create a virtual contact center in the AWS cloud. To get started, create a virtual contact center instance. For more information, see Get started with Amazon Connect.

After you create an instance, you can edit its settings, such as telephony, data storage, and data streaming. After that, you can assign your contact center a phone number or import your own phone number. You can add agents to your contact center, and assign them permissions appropriate to their roles. You can set up a single queue for incoming contacts, or set up multiple queues so that you can route contacts to agents with specific skills.

A key part of setting up your contact center is to define how your customers experience it. You do this by creating flows.

Finally, you’ll need to provide your agents access to the Contact Control Panel (CCP), which they will use to interact with contacts.

Contents

• Create an Amazon Connect instance
• Test voice, chat, and task experiences
• Set up phone numbers to use the Amazon Connect service
• Set up outbound communications
• Manage users in Amazon Connect
• Set up routing
• Set up agents
• Set up tasks
• Set up in-app, web, and video calling capabilities
• Set up your customer's chat experience
• Set up SMS messaging
• Upgrade to the latest CCP
• Provide agents with access to the Contact Control Panel
• Embed a custom Contact Control Panel (CCP)
Create an Amazon Connect instance

The first step in setting up your Amazon Connect contact center is to create a virtual contact center instance. Each instance contains all the resources and settings related to your contact center.

Things to know before you begin

- When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon Connect. You are charged only for the services that you use. To create an AWS account, see How do I create and activate an AWS account?
- To allow a user to create an instance, ensure that they have the permissions granted by the AmazonConnect_FullAccess policy.
- For a list of the minimum IAM permissions required to create an instance, see Required permissions for using custom IAM policies to manage access to the Amazon Connect console.
- Amazon Connect is not available to customers in India using Amazon Web Services through Amazon Internet Services Pvt. Ltd (AISPL). You will receive an error message if you try to create an instance in Amazon Connect.
- When you create an instance, you must decide how you want to manage users. You can't change the identity management option after you create the instance. For more information, see Plan your identity management in Amazon Connect.

Step 1: Set identity

Permissions to access Amazon Connect features and resource are assigned to user accounts within Amazon Connect. When you create an instance, you must decide how you want to manage users. You can't change the identity management option after you create the instance. For more information, see Plan your identity management in Amazon Connect.

To configure identity management for your instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose Get started. If you have previously created an instance, choose Add an instance instead.
3. Choose one of the following options:
   - Store users in Amazon Connect - Use Amazon Connect to create and manage user accounts. You cannot share users with other applications.
• **Link to an existing directory** - Use an AWS Directory Service directory to manage your users. You can use each directory with one Amazon Connect instance at a time.

• **SAML 2.0-based authentication** - Use an existing identity provider (IdP) to federate users with Amazon Connect.

4. If you chose **Store users within Amazon Connect** or **SAML 2.0-based authentication**, provide the left-most label for **Access URL**. This label must be unique across all Amazon Connect instances in all Regions. You can't change the access URL after you create your instance.

5. If you chose **Link to an existing directory**, select the AWS Directory Service directory for **Directory**. The directory name is used as the left-most label for **Access URL**.

6. Choose **Next**.

**Step 2: Add administrator**

After you specify the user name of the administrator for the Amazon Connect instance, a user account is created in Amazon Connect and the user is assigned the **Admin** security profile.

**To specify the administrator for your instance**

1. Do one of the following, based on the option that you chose in the previous step:
   - If you chose **Store users within Amazon Connect**, select **Specify an administrator**, and provide a name, password, and email address for the user account in Amazon Connect.
   - If you chose **Link to an existing directory**, for **Username**, type the name of an existing user in the AWS Directory Service directory. The password for this user is managed through the directory.
   - If you chose **SAML 2.0-based authentication**, select **Add a new admin** and provide a name for the user account in Amazon Connect. The password for this user is managed through the IdP.

2. Choose **Next**.

**Step 3: Set telephony**

Use the options in this section to choose whether you want your agents to receive calls from customers, make outbound calls, and hear early media audio.
Early media

When early media audio is enabled, for outbound calls your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages provided by telephony providers.

Note
The early media feature is not supported for transfers that are dialed through the Transfer to phone number block in flows.

By default, early media is enabled for you. Note the following exception:

- Your instance was created before April 17, 2020, and you weren't enrolled in the preview program. You need to enable early media audio. For instructions, see Update telephony options.

To configure telephony options for your instance

1. To allow inbound calls to your contact center, choose Allow incoming calls.
2. To enable outbound calling from your contact center, choose Allow outgoing calls.
3. To enable multi-party calls, choose Enable up to six parties on a call.
4. Choose Next.

Step 4: Data storage

Note
Amazon Connect does not support Amazon S3 Object Lock in compliance mode to store objects using a write-once-read-many (WORM) model.

When you create an instance, by default we create an Amazon S3 bucket. Data, such as reports and recordings of conversations, is encrypted using AWS Key Management Service, and then stored in the Amazon S3 bucket.
This bucket and key are used for both recordings of conversations and exported reports. Alternatively, you can specify separate buckets and keys for recordings of conversations and exported reports. For instructions, see Update instance settings.

By default, Amazon Connect creates buckets for storing call recordings, chat transcripts, exported reports, and flow logs.

- When a bucket is created to store call recordings, call recording is enabled at the instance level. The next step for setting up this functionality is to set up recording behavior in a contact flow.
- When a bucket is created to store chat transcripts, chat transcription is enabled at the instance level. Now all chat transcripts will be stored. Only if you want to monitor chat conversations do you need to set up recording behavior in a contact flow.
- Live media streaming is not enabled by default.
- Screen recording is not enabled by default. For more information, see Enable screen recording.

By default, Amazon Connect creates a Customer Profiles domain, which stores profiles that combine customer contact history with customer information such as account number, address, billing address, and birth date. Data is encrypted using AWS Key Management Service. You can configure Customer Profiles to use your own customer managed key after your instance is set up. For more information, see Create a KMS key to be used by Customer Profiles to encrypt data (required).

Review and copy the location of the S3 bucket, flow logs, and whether you want to enable Customer Profiles.

1. If desired, copy the location of the S3 bucket where your data encryption is stored, and the location of the flow logs in CloudWatch.
2. Choose Next.

Step 5: Review and create

To create your instance

1. Review the configuration choices. Remember that you cannot change the identity management options after you create the instance.
2. (Optional) To change any of the configuration options, choose Edit.
3. Choose **Create instance**.

4. (Optional) To continue configuring your instance, choose **Get started** and then choose **Let's go**. If you prefer, you can access your instance and configure it later on. For more information, see [Next steps](#).

If you chose to manage your users directly within Amazon Connect or through an AWS Directory Service directory, you can access the instance using its access URL. If you chose to manage your users through SAML-based authentication, you can access the instance using the IdP.

**Next steps**

After you create an instance, you can assign your contact center a phone number or import your own phone number. For more information, see [Set up phone numbers to use the Amazon Connect service](#).

**Create a dev (Sandbox) or test (QA) instance**

You might want to create multiple contact center instances, for example, one as a Sandbox for development, another for QA, and a third for Production.

Each instance functions only within the AWS Region in which you create it.

⚠️ **Important**

Most entities in Amazon Connect can be (re)created and replicated among instances using the Amazon Connect API. While doing that keep the following limitations in mind:

- Service quotas are specific to each instance.
- Some supporting services, such as User Directory, can be linked to only one Amazon Connect instance at a time.
- Any additional external and Region-specific limitations.

For more information, see [Can I migrate my Amazon Connect instance from a test environment to a production environment?](#)
To create another instance

1. In the AWS Management Console, choose Amazon Connect.
2. Choose Add an instance.
3. Complete the steps on the Amazon Connect resource configuration page. For instructions see Create an Amazon Connect instance.

Find your Amazon Connect instance ID/ARN

When you open a support ticket, you may be asked to provide your Amazon Connect instance ID (also called the ARN). Use the following steps to find it.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

On the Account overview page, in the Distribution settings section, you can see the full instance ARN.
The information after instance/ is the instance ID.

Find your Amazon Connect instance name

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, the instance name appears in the Instance Alias column. This instance name appears in the URL you use to access Amazon Connect.

Update instance settings

To update the instance settings:

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. Complete the following procedures.

**Update telephony options**

1. In the navigation pane, choose **Telephony**.
2. To enable customers to call into your contact center, choose **Receive inbound calls with Amazon Connect**.
3. To enable outbound calling from your contact center, choose **Make outbound calls with Amazon Connect**.
4. To enable outbound campaigns, choose **Enable outbound campaigns**.
5. By enabling early media audio, your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages from telephony providers, when making outbound calls. Choose **Enable early media**.

   **Note**
   
   The early media feature is not supported for transfers that are dialed through the **Transfer to phone number** block in flows.

6. By default, you can have three participants on a call (for example, two agents and a customer, or an agent, a customer, and an external party). To enable multi-party calls with more participants, choose **Enable up to six parties on a call**. This feature is only available in CCPv2.
7. Choose **Enable Multi-Party Calls and Enhanced Monitoring**. This setting is required to use the barge feature. See **Barge live conversations**.
8. Choose **Save**.
Update data storage

- In the navigation pane, choose **Data storage**. Choose the following:
  - **Call recordings**: Choose **Edit**, specify the bucket and KMS key for recordings of voice conversations, and then choose **Save**.

    When this bucket is created, call recording is enabled at the instance level. The next step for setting up this functionality is to [set up recording behavior in a flow](#).
  - **Chat transcripts**: Choose **Edit**, specify the bucket and KMS key for recordings (transcripts) of chat conversations, and then choose **Save**.

    When this bucket is created, chat transcripts are enabled at the instance level. Now all chat transcripts will be stored here.
  - **Live media streaming**: Choose **Edit** to enable live media streaming, choose **Edit**. For more information, see [Set up live media streaming of customer audio](#).
  - **Exported reports**: Choose **Edit**, specify the bucket and KMS key for exported reports, and then choose **Save**.
  - **Attachments**: Choose **Edit**, then **Enable Attachments sharing** to enable file sharing for both agents and customers. For more information about this option and additional steps, see [Enable attachments to share files using chat and upload files to cases](#).
  - **Contact evaluations**: Choose **Edit**, specify the bucket and KMS key for performance evaluations, and then choose **Save**.

    When this bucket is created, evaluations are enabled at the instance level. The next step for setting up this feature is to [create an evaluation form](#).
  - **Screen recordings**: Choose **Edit**, specify the bucket and KMS key for recordings of agent screens, and then choose **Save**.

    When this bucket is created, screen recording is enabled at the instance level. The next step for setting up this functionality is to download and install the agent app, and then enable screen recording in the Set recording and analytics behavior block. For more information, see [Enable screen recording](#).

Update data streaming options

1. In the navigation pane, choose **Data streaming**.
2. Choose **Enable data streaming**. For more information, see [Enable data streaming for your instance](#).

3. For **Contact records**, do one of the following:
   - Choose **Kinesis Firehose** and select an existing delivery stream, or choose **Create a new Kinesis Firehose** to open the Kinesis Firehose console and create the delivery stream.
   - Choose **Kinesis Stream** and select an existing stream, or choose **Create a new Kinesis Firehose** to open the Kinesis console and create the stream.

4. For **Agent Events**, select an existing Kinesis stream or choose **Create a new Kinesis Stream** to open the Kinesis console and create the stream.

5. Choose **Save**.

**Update analytics tools options**

1. In the navigation pane, choose **Analytics tools**.

2. Choose **Enable Contact Lens**. For more information, see [Analyze conversations using conversational analytics](#).

3. Choose **Save**.

**Update flow settings**

1. In the navigation pane, choose **Flows**.

2. (Optional) To add a signing key for use in flows, choose **Add key**. For more information, see [Encrypt customer input](#).

3. (Optional) To integrate with Amazon Lex, select a Lex bot. For more information, see [Add an Amazon Lex bot to Amazon Connect](#).

4. (Optional) To integrate with AWS Lambda, select a Lambda function. For more information, see [Invoke AWS Lambda functions](#).

5. (Optional) To enable flow logs, choose **Enable flow logs**. For more information, see [Track events as customers interact with flows](#).

6. (Optional) To use the best available voice from Amazon Polly, choose **Use the best available voice**. For more information, see [Amazon Polly best sounding voice](#).

7. (Optional) Use the voices available in Amazon Polly.
Enable attachments to share files using chat and upload files to cases

You can allow customers and agents to share files using chat, and allow agents to upload files to cases. After you complete the steps in this topic, an attachment icon automatically appears in your agent's Contact Control Panel so they can share attachments on chats.

For a list of supported file types, see Amazon Connect feature specifications.

If you are not using the hosted communications widget, you need to update your customer-facing chat interfaces to support attachment sharing.

Using a custom agent application? Check out the APIs we've added to support attachment sharing: StartAttachmentUpload, CompleteAttachmentUpload, and GetAttachment.

Step 1: Enable attachments

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. On the Data storage page, under the Attachments, choose Edit, select Enable Attachments sharing, and then choose Save.

   Storage options appear, similar to the following image.
4. You can change the Amazon S3 bucket location where attachments are stored. By default, your existing Amazon Connect bucket is used, with a new prefix for attachments.

**Note**
Currently, Amazon Connect doesn't support S3 buckets with Object Lock enabled.

The attachments feature leverages two Amazon S3 locations: a staging location and a final location.

Note the following about the staging location:

- The staging location is used as part of a business validation flow. Amazon Connect uses it to validate the file size and type before it is shared with the chat participant.
• The staging prefix is created by Amazon Connect based on the bucket path you have selected. Specifically, it includes the S3 prefix for where you are saving files, with staging appended to it.

• We recommend that you change the data retention policy for the staging prefix to one day. This way you won't be charged for storing the staging files. For instructions, see How do I create a lifecycle rule for an S3 bucket? in the Amazon S3 User Guide.

Warning
Only change the lifecycle for the file staging location. If you accidentally change the lifecycle for the entire Amazon S3 bucket, all transcripts and attachments will be deleted.

Step 2: Configure a CORS policy on your attachments bucket

To allow customers and agents to upload and download files, update your cross-origin resource sharing (CORS) policy to allow PUT and GET requests for the Amazon S3 bucket you are using for attachments. This is more secure than enabling public read/write on your Amazon S3 bucket, which we don't recommend.

To configure CORS on the attachments bucket

1. Find the name of the Amazon S3 bucket for storing attachments:
   a. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
   b. In the Amazon Connect console, choose Data storage, and locate the Amazon S3 bucket name.
2. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
3. In the Amazon S3 console, select your Amazon S3 bucket.
4. Choose the Permissions tab, and then scroll down to the Cross-origin resource sharing (CORS) section.
5. Add a CORS policy that has one of the following rules on your attachments bucket. For example CORS policies, see Cross-origin resource sharing: Use-case scenarios in the Amazon S3 Developer Guide.
• Option 1: List the endpoints from where attachments will be sent and received, such as the name of your business web site. This rule allows cross-origin PUT and GET requests from your website (for example, http://www.example1.com).

Your CORS policy may look similar to the following example:

```
[
  {
    "AllowedMethods": [
      "PUT",
      "GET"
    ],
    "AllowedOrigins": [
      "http://www.example1.com",
      "http://www.example2.com"
    ],
    "AllowedHeaders": [
      "*"
    ]
  }
]
```

• Option 2: Add the * wildcard to AllowedOrigin. This rule allows cross-origin PUT and GET requests from all origins, so you don’t have to list your endpoints.

Your CORS policy may look similar to the following example:

```
[
  {
    "AllowedMethods": [
      "PUT",
      "GET"
    ],
    "AllowedOrigins": [
      "*
    ],
    "AllowedHeaders": [
      "*"
    ]
  }
]
```
Step 3: Update your chat UI

To help you update the chat user interface that your customers use, we’ve posted an updated version of chat interface JS. It exposes an attachment icon on the UI and supports the backend calls for attachment sharing. See Amazon Connect Chat UI Examples on GitHub.

Next step

We recommend enabling attachment scanning to meet compliance requirements or security policies that your organization may have in place for file sharing. For more information, see Set up attachment scanning.

Attachments not appearing?

If your agents report problems receiving and sending attachments in chat messages, see Internal firewall prevents access to chat or case attachments.

Set up attachment scanning

Note

This topic is for developers who are familiar with Lambda. If you're new to Lambda, see Getting started with Lambda in the AWS Lambda Developer's Guide.

You can configure Amazon Connect to scan attachments that are sent during a chat or uploaded to a case. You can scan attachments by using your preferred scanning application. For example, you can scan attachments for malware before they are approved to be shared between participants of a chat.

To enable attachment scanning you perform two steps:

- Configure a Lambda function that calls your preferred scanning application.
- Add the scanner to your Amazon Connect instance.

Step 1: Create a Lambda function that handles scanning

Create a Lambda function, using any runtime, and configure it. This function must be in the same AWS Region and account as your Amazon Connect instance.
For every attachment uploaded through Amazon Connect a request is sent with information about the attachment.

Following is an example JSON request for scanning:

```json
{
    "Version": "1.0",
    "InstanceId": "your instance ID",
    "File": {
        "FileId": "your file ID",
        "FileCreationTime": 1689291663582,
        "FileName": "example.txt",
        "FileSizeInBytes": 10,
        "FileLocation": {
            "S3Location": {
                "Key": "connect/your-instance/Attachments/chat/2023/07/13/your file ID_20230713T23:41_UTC.txt",
                "Bucket": "connect-example",
                "Arn": "arn:aws:s3:::connect-example/connect/your-instance/Attachments/chat/2023/07/13/your file ID_20230713T23:41_UTC.txt"
            }
        }
    }
}
```

**Required response**

```json
{
    "Status": "APPROVED" | "REJECTED"
}
```

**Invocation retry policy**

If your Lambda invocation gets throttled, the request is retried. It is also retried if a general service failure (500 error) happens. When a synchronous invocation returns an error, Amazon Connect retries up to 3 times, for a maximum of 60 seconds. At that point, the attachment is marked rejected.

For more information about how Lambda retries, see [Error handling and automatic retries in AWS Lambda](https://docs.aws.amazon.com/lambda/latest/dg/error-handling-automatic-retries.html).
Rejection behavior

Amazon Connect marks the attachment REJECTED and automatically deletes attachment files in S3 from both staging and final locations when one of the following occurs:

- Your Lambda scanner returns a status of REJECTED.
- Amazon Connect is unable to parse the response from the Lambda scanner.
- Amazon Connect is unable to invoke the Lambda function.

Step 2: Add an attachment scanner to your Amazon Connect instance

After you create a Lambda for attachment scanning, you need to add the Lambda to your Amazon Connect instance. Perform the following steps to add the Lambda.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose Data storage.
4. On the Data storage page, in the Attachments section, choose Edit, and then select Enable attachments scanning, as shown in the following image.
5. Use the **Lambda Functions** drop-down box to select the Lambda function that you added in *Step 1: Create a Lambda function that handles scanning*.

6. Choose **Save**. Attachment scanning is now enabled for your Amazon Connect instance.

**Enable data streaming for your instance**

You can export contact records and agent events from Amazon Connect and perform real-time analysis on contacts. Data streaming sends data to Amazon Kinesis.

**To enable data streaming for your instance**

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).

2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL. The following image shows the **Amazon Connect virtual contact center instances** page, with a box around the instance alias.

3. In the navigation pane, choose **Data streaming**.

4. Choose **Enable data streaming**.

5. For **Contact records**, do one of the following:
• Choose **Kinesis Firehose** and select an existing delivery stream, or choose **Create a new Kinesis firehose** to open the Kinesis Firehose console and create the delivery stream. For more information, see [Creating an Amazon Kinesis Data Firehose Delivery Stream](#).

• Choose **Kinesis Stream** and select an existing stream, or choose **Create a Kinesis stream** to open the Kinesis console and create the stream. For more information, see [Creating and Managing Streams](#).

6. For **Agent Events**, select an existing Kinesis stream or choose **Create a new Kinesis stream** to open the Kinesis console and create the stream.

7. Choose **Save**.

---

## Using server-side encryption for the Kinesis stream

If you enable server-side encryption for the Kinesis stream you select, Amazon Connect cannot publish to the stream because it does not have permission to call `kms:GenerateDataKey` so that it can encrypt data sent to Kinesis. To work-around this, do the following steps:

1. Enable encryption for recordings of conversations or scheduled reports.
2. Create a customer managed key to use for encryption.
3. Choose the same customer managed key for the Kinesis data stream that you use for scheduled reports or recordings of conversations.

   For more information, see [Creating Keys](#) in the **AWS Key Management Service Developer Guide**.

---

## Emergency admin login

As a best practice, users assigned to the Amazon Connect **Admin** security profile should always use their Amazon Connect instance URL to login:

- Log in to the Amazon Connect admin website at `https://instance name.my.connect.aws/`.

This method ensures the appropriate levels security.

However, if there's an emergency, you can log in from the Amazon Connect console using your AWS account credentials. For example, you may need to login in this way in the following situations:
• You forgot your Amazon Connect administrator password and no other Amazon Connect administrators are around to reset it.

• Someone deleted the Amazon Connect Admin security profile by mistake.

To login for emergency access

1. Make sure you have your AWS account credentials at hand and that you have the required permissions.

2. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

3. If prompted to login, enter your AWS account credentials.

4. Choose the name of the instance from the Instance alias column.

5. In the navigation pane, choose Overview.

6. Choose Log in for emergency access.

You aren't prompted for your credentials because you are federated in from the AWS console.

⚠️ Important

For daily usage, we strongly recommend always using your instance URL to login. The procedure provided in this article should only be used for emergency access when using the instance URL is not an option.

To log out

To log out of your instance, go to the title bar at the top of the screen and select the icon with the arrow (Log out) that appears next to your user name.
Delete your Amazon Connect instance

If you no longer need your Amazon Connect instance, you can delete it. Here's what happens when you delete it:

- Its claimed phone number is released back to inventory.
- When customers call the phone number that you've released, they'll get a message that it's not a working phone number.

⚠️ **Important**

You can't restore a deleted Amazon Connect instance or access its settings, data, metrics, and reports.

Delete your instance

You must have the appropriate AWS permissions to delete an Amazon Connect. If your organization is using IAM, see [Required permissions for using custom IAM policies to manage access to the Amazon Connect console](https://console.aws.amazon.com/connect/).

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).
2. Select the radio button for the instance.
3. Choose Delete. If you don't see the Delete button, you don't have permissions to delete instances. Contact your AWS administrator for help.

4. When prompted, enter the name of the instance and then choose Delete.
Tip

We recommend checking your CloudWatch log groups related to the Amazon Connect instance, and deleting them if they are no longer needed. For more information, see Delete a CloudWatch Logs log group using an AWS SDK.

Error message: "Region Unsupported. Amazon Connect is not available in [Region]"

If you get this error message, it means that you selected a Region in the AWS Management Console that is not the Region in which you created the Amazon Connect instance, and Amazon Connect isn't available in that Region.

To switch Regions and delete your Amazon Connect instance

1. From the navigation bar, open the Region selector. Select the Region in which you created the Amazon Connect instance.

<table>
<thead>
<tr>
<th>Region</th>
<th>Region Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
</tr>
<tr>
<td><strong>US East (Ohio)</strong></td>
<td><strong>us-east-2</strong></td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>us-west-1</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>ap-east-1</td>
</tr>
<tr>
<td>Asia Pacific (Jakarta)</td>
<td>ap-southeast-3</td>
</tr>
</tbody>
</table>

2. From the navigation bar, choose Amazon Connect from the list of services to open the Amazon Connect console. If you don't see the instance, keep selecting from the supported Regions until you find your instance.
3. Select the radio button for the instance.

4. Choose **Delete**. If you don't see the **Delete** button, you don't have permissions to delete instances. Contact your AWS administrator for help.

5. When prompted, enter the name of the instance and then choose **Delete**.

### Test voice, chat, and task experiences

To learn what the voice, chat, and task experiences are like for your agents and customers, you can test them without doing any development.

#### Test voice

At the basic level, after you claim a number you can immediately call it to hear what the experience will be like for your customers. Amazon Connect uses the default flows to power your initial experience.

To test a customized flow, assign a phone number to it and then call that number.

**Tip**

Call latency significantly impacts the quality of your customer's experience. For guidance about designing your contact center for optimal call quality and then testing latency, see [Ensure call quality: Design your contact center for low latency](#).

#### Test chat

Amazon Connect includes a simulated web page that shows how your customers can interact with you, and a Contact Control Panel (CCP) that shows the agent experience. Here's how to test chat:

1. On the navigation menu, choose **Dashboard**, as shown in the following image.
2. Choose Test chat.

If you don't see the option to test chat, click here.

3. On the Test Chat page, choose Test Settings.

4. Under System Settings, choose the flow you want to test with chat, and then click Apply. By default, it runs the Sample inbound flow.

Tip
If you want to test a chat and use contact attributes, note that the key and value pair must be enclosed in quotes, as shown in the following image:

5. In the chat window, click the icon as shown in the following image.
6. Type a message similar to what one of your customers might type. In the agent window, type a reply.

7. To see what it's like for an agent to handle multiple chat conversations, copy the dashboard URL into another browser window, and start another chat. The chat goes to the same instance of the CCP that you already have open.

   **Tip**
   The test environment uses the BasicQueue and Basic Routing Profile. The Basic Routing Profile is set up for 2 chats. If you want to test what it's like to have more than two chats, change the Basic Routing Profile to 5 chats. For instructions, see [Create a routing profile](#).

To learn more about what the agent experiences when managing chat conversations, see [How to use the CCP to manage chats](#).

**Test tasks**

The first step in testing the task experience is to create a quick connect for the queue you want to assign the example tasks to.

**Step 1: Create a quick connect**

1. On the navigation menu, choose **Routing, Quick connects, Add a new**.

2. Enter a name for the quick connect. For example, if you want to assign the test task to yourself, enter your name (for example, **Jane Doe**).
3. Under **Type**, use the dropdown list to choose **Queue**.

4. Under **Destination**, use the dropdown list to choose a queue you set up for yourself (assuming you want to assign the test task to yourself).

5. Under **flow**, choose **Default queue transfer**.

6. Under **Description**, enter something like **Test quick connect**.

7. Choose **Save**. The completed quick connect looks similar to the quick connect in the following image.

![Quick connects](image)

**Step 2: Make the quick connect visible in the CCP by assigning it to a queue**

1. After you create the quick connect, go to **Routing, Queues** and then choose the appropriate queue for the contact to be routed to.

2. On the **Edit queue** page, in the **Quick connects** box, search for the quick connect you created. For example, it might have your name. The following image shows the quick connect for Jane Doe.
3. Select the quick connect and then choose **Save**.

**Step 3: Assign the queue to the agent's routing profile**

1. Go to **Users, Routing profiles** and choose the agent's routing profile.
2. Under **Set channels and concurrency** choose **Tasks**.
3. Add the agent's queue to the routing profile, and choose **Task** for the channel.

   If the agent can receive transfers through other channels, select them as well.
4. Choose **Save**.
Step 4: Test tasks

1. Open the CCP. Select the **Task** tab, and then choose **Create task**. The following image shows there are two ways to choose **Create task**: choose the task icon in the top right corner, or choose the **Create task** button at the bottom of the CCP page.

![Create task image]

Or, if you're testing the chat experience, for example, you can choose the **Task** icon, as shown in the following image.

![Chat task image]
2. Complete the **Create task** page. When you choose **Assign to**, you can assign only a task to someone or a queue that has quick connect.

To create a scheduled task for the future, use the **Scheduled date/time** box to choose a future date and time. You can schedule a task up to six days in future.

Choose **Create**.
3. If you chose yourself, the task will be routed to you. The following image of the CCP shows what it looks like when a task arrives. Choose Accept task.
4. Review the task. When you're done with the task, choose **End task** when done.
View metrics for the test experiences

When you're testing the voice, chat, and task experiences, you may also want to explore metrics.

1. On the left navigation menu, choose Analytics and optimization, Real-time metrics, Queues.
2. You can review the real-time metrics as you test the different channels.
3. To view metrics by channel in a real-time metrics report, go to Settings, Groupings, Queues grouped by channels, Apply. Your report will look similar to the following image.

![Customer follow up task](https://example.com)
## Set up phone numbers to use the Amazon Connect service

⚠️ **Important**

If you found this page because you need to contact Amazon for support, see [Amazon Customer Service](#) (Amazon orders and deliveries) or [AWS Support](#) (Amazon Web Services).

After you create an Amazon Connect instance, you can claim a phone number to use for your contact center. You can use this phone number to place a test call in to your contact center to confirm that it is working correctly. You can also use it in your production environment.

- For pricing information about claimed phone number costs, see [Amazon Connect pricing](#).
- For a list of the telephony capabilities that Amazon Connect provides, see the [Amazon Connect Telecoms Country Coverage Guide](#).

If you want to keep a phone number you already have, you can port the phone number and use it with Amazon Connect. After a phone number is ported to Amazon Connect, it appears in the list of available phone numbers for you to assign to flows.
Port your current phone number to Amazon Connect

You can port your existing phone numbers to your Amazon Connect contact center.

Contents

- Things to know before porting a phone number to Amazon Connect
- Things to know about South Korean numbers, regulations, and porting
- Porting your phone numbers
- After the porting process completes

Things to know before porting a phone number to Amazon Connect

The topics in this section explain which numbers can be ported, how long it takes, and what fees you might incur.

Contents

- What is phone number porting?
- How much does number porting cost?
- Can my number be ported to Amazon Connect?
What is phone number porting?

Porting a phone number is the process of moving a phone number from one telephony service provider, or carrier, to another. Many businesses and organizations already have a phone number that is advertised to their customers, so changing this number would be disruptive.

If you port a phone number from your current carrier to Amazon Connect, you can keep using the same phone number for your contact center. This helps to eliminate the need to update your business contact information.

Downtime and service disruption during the porting process

The porting process requires the losing carrier to remove your number from their systems, the winning carrier to add your number to their systems, and for number routing to be updated. Most porting activities complete within 15-30 minutes, with possible call disruptions. To ensure that they have engineers available to troubleshoot issues, most losing carriers complete porting actions only during normal business hours. Carriers typically communicate a two-hour porting window to resolve any issues that could arise.

For detailed information about available porting dates and times, see Region requirements for ordering and porting phone numbers for your country or region.

What happens to a number after it is ported

As long as you continue to pay for the phone number, and do not release it from your Amazon Connect instance, it stays assigned to your account, and you are billed accordingly.

To release a phone number, follow the steps in Release a phone number from Amazon Connect back to inventory.

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.
If you move your contact center away from Amazon Connect, and want to port your phone number away from Amazon Connect, see Port phone numbers away from Amazon Connect.

**How much does number porting cost?**

Amazon Connect does not charge fees for porting numbers. Your existing carrier may have fees associated with the disconnection and early termination of your service.

After a phone number is ported to Amazon Connect, standard pricing applies for Amazon Connect service usage and associated telephony rates.

**Can my number be ported to Amazon Connect?**

Not all phone numbers can be ported. The ability to port a specific phone number depends on several factors. For example:

- The regulations in the country or region of the phone number.
- Agreements between the losing and winning carriers.
- The type of phone number being ported.
- Your service contract with your current service provider.

To find out if a phone number that you currently own—whether local, mobile, or toll-free—can be ported to Amazon Connect:

1. See if your country or region supports number porting: Region requirements for ordering and porting phone numbers.
2. Then get started by submitting an Amazon Connect support ticket for number verification.

**Porting numbers purchased from other contact center providers**

In most cases, you can port numbers that were purchased from other contact center providers. Confirm with your current contact center provider who holds the assignment to the number, and work with them to ensure the correct information is provided in the Letter of Authorization (LOA).

**Port short phone numbers**

Because of Telecom regulations in various countries or regions, the short phone number will need to be evaluated on a case-by-case basis. To verify if your phone number can be ported to Amazon Connect, submit an Amazon Connect support ticket.
Port a number to one EU Region only

The Amazon Connect Regions of EU-CENTRAL-1 and EU-WEST-2 are symmetrical European Regions that offer the same carrier coverage for telephony. If a phone number cannot be ported to an instance in one of these Regions, then it cannot be ported to an instance in the other.

If you had a phone number ported into the EU-CENTRAL-1 or EU-WEST-2 Regions, and want to move it to the other Region, submit an Amazon Connect support ticket for assistance.

The same is true for the North America Regions of US-EAST-1 and US-WEST-2.

Port a subset of numbers from a block

If you have a block of numbers, in some instances Amazon Connect can port a subset or portion of your phone numbers. In other cases, it is required by the carrier to port full block of phone numbers.

If you want to port only a subset of the phone numbers you currently own to Amazon Connect, submit an Amazon Connect support ticket to verify whether the phone numbers can be ported. We will verify the actions that can be completed and assist you with next steps.

Note

If you port only a subset of the phone numbers, you will still be liable for the remaining phone numbers with the original carrier and any associated fees.
If your intent to is release the remaining phone numbers not being ported to Amazon Connect, we recommend waiting until the requested porting has been completed to avoid any disruptions to service.

Letter of compromise

Before porting phone numbers, some customers ask for a letter of compromise stating that they will be allowed to move their phone numbers from Amazon Connect to another service, if their contact center moves. Because of Telecom regulations in various countries, the phone number will need to be evaluated on a case-by-case basis. To verify that your phone number can be ported to Amazon Connect, submit a ticket to Amazon Connect support.
How long does it take to port numbers?

⚠️ **Important**

Open a porting request as far in advance of your pending go-live date as possible.

The amount of time that it takes to port numbers depends on the country, complexity of the request, the type and quantity of numbers being ported, and your current carrier. Telecom carriers also may implement porting block days because of holidays and network maintenance. Because of this, Amazon Connect requires porting requests to be open several months before pending go-live dates.

For a list of countries and their portability windows, see [Region requirements for ordering and porting phone numbers](#).

### Inside the US and Canada

Phone numbers in the US or Canada typically take between two to four weeks to port, after phone number portability has been verified, and all required documents are correctly submitted to the carrier.

### Outside the US and Canada

Phone numbers outside the US and Canada require between two to six months to complete the full porting process. This includes:

- Time for you to submit all the documents to AWS Support.
- Time for the Amazon Connect service provider to verify whether they can port all of the phone numbers that you have requested.
- Time for the losing provider to verify the provided documents.

After all documents are verified by the losing provider, the losing provider and the Amazon Connect service provider will schedule a mutually agreed date to port the numbers to Amazon Connect.
What affects porting timelines?

Porting timelines can be negatively impacted when incorrect information is provided on the required Letter of Authorization (LOA). This causes the LOA to be rejected and resets the porting timelines.

Port many numbers over multiple countries or carriers

Complex porting requests have their own timelines. The timelines discussed elsewhere in this topic do not apply to complex porting requests.

Complex porting requests for more than 10 distinct number ranges or 10 distinct locations are considered a project and require advanced coordination with your AWS Account team. If you are a Business or Enterprise customer, engage your Amazon Connect Solutions Architect (SA) or Technical Account Manager (TAM) for assistance in planning your number porting.

To help make the process as smooth as possible, gather the following information before submitting a porting request:

- Your most recent telephony bill from the carriers that currently service the numbers to be ported.
- The country specific documentation required; see Region requirements for ordering and porting phone numbers.
- The contact information for a central point of contact who can act on behalf of your organization in support of the porting requests.

Can I choose the port date?

Depending on the country and carriers involved, you may be able to choose the porting date and time. In most cases, however, the losing carrier picks the date and time and communicates it to Amazon Connect based on their schedule.

If you have a specific date and time you want to request, provide the information in your support case. We will work with our carrier to determine if they can support the requested date and time.
Note
Most carriers only support porting activity during their normal business hours. For detailed information about available porting dates and times for your country, see Region requirements for ordering and porting phone numbers.

Can I cancel a porting that is already scheduled?

Important
If you need to cancel or reschedule your porting, let us know immediately.

Depending on the country of service, after a mutually agreed date and time has been provided it can be difficult to cancel.

Because of the coordination required between carriers, Amazon Connect support requires a minimum of 5 business days notice to cancel or reschedule a porting request, if the number has not already been ported. If you need to cancel or reschedule your porting, let us know immediately.

You cannot cancel a port after it has been moved to the RespOrg (Responsible Organization). The port is complete. For this situation, see Revert to original carrier after porting.

If a porting is successfully cancelled, timelines for the port schedule are reset and the carriers will need to identify another mutually agreed date and time. This will impact the overall timeline for porting your numbers.

Note
Please be advised that sometimes a porting request cannot be cancelled because of process automation, but Amazon Connect support will make every attempt possible to stop the request.

When do I cancel my current telecom service?

Do not cancel your existing telecom service until your phone numbers have been ported and confirmed working in Amazon Connect.
Canceling your existing telecom service before your number is ported releases your phone number assignment, and may result in you losing the number.

**Things to know about South Korean numbers, regulations, and porting**

Rules for South Korea differ from those in other countries. To help with requirements in South Korea, here are some helpful hints.

- When planning your Amazon Connect project in South Korea one of the most important things you will need to do is plan and request information up front. To port numbers in South Korea, you may need to complete and submit more than 5 forms and you may need to engage with the local regulatory authority before approvals are granted to port numbers.

- All geographic numbers (that is, other than toll-free, national, representative, or 070 VOIP) must be in place on a physical termination for a minimum of 6 months before they can be ported into Amazon Connect. However, if a number has been in place for a minimum of 3 months, you can port it by filing a special request with the Korean Ministry of Telecommunications; upon approval, the porting process can begin. Amazon Connect can provide you with the forms, but you must complete and submit them to the regulator directly.

- All geographic, representative, or toll-free numbers (GRTFN) are assigned a 070 VOIP number to which the GRTFN terminates and which are associated with the GRTFN at the carrier. Do not remove this 070 number from your Amazon Connect instance until the related GFTN number is removed. If you do, all inbound and outbound calls will fail.

- Representative numbers (RN) have minimum session billing requirements based on the "attractiveness" of the RN, as determined by the carrier. These minimums range from 2 to 500 Special Number sessions. While the RN is associated with a single "normal" 070 DID, each minimum session will be billed as a Special Number DID. These additional Special Number DIDs do not have the ability to be assigned call flows, and outbound calls from them will fail. If you disconnect RNs, be sure to also remove their associated Special Numbers to avoid future billing. Removal or reduction of Special Number DIDs without removal of the underlying RN is a violation of Amazon Connect Terms of Service.

- Amazon Connect is currently in beta with outbound from Representative numbers. If you have outbound requirements, raise a request to your account team because it requires additional setup.
Porting your phone numbers

Porting phone numbers from your existing carrier to Amazon Connect is a multi-step process. It's important to get started several months in advance of your scheduled go-live date, and have all of your documentation in order.

Contents

• How to port your numbers to Amazon Connect
• Documentation requirements for porting numbers
• How to verify flows before numbers are ported

How to port your numbers to Amazon Connect

⚠️ Important

Starting Friday, December, 01, 2023, Amazon Connect phone number porting requests will move to the Account and billing section of the AWS Support Center console. To create a new support case for phone number porting, you will choose Account and billing, and then choose Amazon Connect (Number Management) from the Services dropdown menu.

The following steps are for a typical porting request. This process requires timely communication to make progress. If you take longer than 30 days to respond to requests for information, your porting request may be cancelled, rescheduled, or restarted from the beginning. For a list of country-specific requirements for porting numbers, see Region requirements for ordering and porting phone numbers.

Step 1: Submit an Amazon Connect support ticket

1. Choose Account and billing to go to the pre-populated form in the AWS Support console. You must be signed in to your AWS account to access the form.

2. For Service, Connect (Number Management) should be selected.

3. For Category, Number Porting North America (US/Canada/Mexico) or Number Porting Non-North America should be selected.

4. Select the required severity.

5. Choose Next step: Additional information

6. On the Additional information page:
a. Enter the subject.

b. Under **Description**, include as much information as possible about your request, including phone number(s) to be ported, your current carrier, and the contact information for the person authorized to make changes to your current phone service. If you don’t know all of these details, you can leave information out.

c. Attach any relevant documents, for example, the invoice of the phone numbers to be ported.

7. Choose **Next step: Solve now or contact us**.

8. On the **Solve now or contact us** page:

   • Choose the **Contact us** tab and select your **Preferred contact language** and your preferred contact method.

9. Choose **Submit**.

10. The Amazon Connect team will review your ticket and get back to you.

### Step 2: Complete Letter of Authorization (LOA)

If the phone number qualifies for porting, the Amazon Connect team will provide you a Letter of Authorization (LOA) to be completed by you. Complete all mandatory fields and sign the LOA.

Along with the LOA, Telecom regulations in many countries require additional documents to register a number, such as proof of business, proof of address, and proof of ID. For a list of country-specific requirements for porting numbers, see [Region requirements for ordering and porting phone numbers](#).

### How to complete an LOA

All portings require the completion of a Letter of Authorization (LOA). The LOA authorizes your current carrier to release your number and allow it to be ported.

- If you are porting multiple numbers from different carriers and countries, submit separate tickets for each set of phone numbers to be ported from different carriers and different countries to streamline communications, tracking, and the LOA process.
- A separate LOA is required for numbers from each losing carrier.

To complete an LOA, provide the following information:
• The numbers to port.

• Information about your current carrier, such as their business name and contact information.

• Contact information for the person authorized to make changes to your phone service. The name, address, and information you provide on the LOA must match the information on file with your current carrier exactly. To help ensure the porting process goes smoothly, include a copy of the Customer Service Record (CSR) or latest phone bill from your carrier. This will have your name, address, and related telephone numbers on it. Check that the information on your LOA matches your CSR exactly.

• If you have any questions regarding specific details about your current service, consult with your current carrier to ensure the data is accurate. This will minimize the risk that the LOA is rejected.

⚠️ Important

Your LOA form must meet the following criteria:

• It must be legible: clearly written or typed.

• It must list your company name, the company address, and contact name. This information must match what is on the current carrier's CSR.

• It must include a true signature. Most carriers will reject an electronic or printed signature.

• It must be dated within the last 15 days.

• If you also want to port toll-free numbers, it must include them as well. Up to 10 toll-free numbers can be listed on the LOA. If you are requesting more than 10 phone numbers be ported, a spreadsheet is required to be attached. Specify "See Attached" on the LOA where the phone numbers would be listed.

• It must include only those telephony numbers that belong to the same current carrier and in the same country. If you have multiple current carriers and countries, you will need to submit multiple LOAs.

To further minimize the risk of having your LOA rejected, see Common reasons why carriers reject an LOA.
Step 3: The porting request goes to the Amazon Connect carrier

After you have submitted all required documentation, the Amazon Connect team submits the porting request on your behalf to the winning carrier.

- The losing and winning carrier follow an industry standard process to validate the contents of the LOA and submitted documentation.
- If the LOA contains discrepancies, it will be rejected and you will need to fix the discrepancies and submit a new LOA.
- After the carriers successfully validate the LOA, they will either confirm your requested date or provide an available date for the actual porting. This is known as the "mutually agreed date."

**Note**

Most carriers require that portings are completed during normal business hours. For country-specific business hours, see [Region requirements for ordering and porting phone numbers](#).

Step 4: Assign the phone number to the flow, request service quota increases

About 3-4 days before the mutually agreed date and time, the Amazon Connect support team loads the phone number that will be ported into the instance ARN you have provided, and then notifies you. Now it's time for you to perform the following steps:

1. **Associate the phone number to the desired flow** so the phone number will be ready to receive phone calls after the porting is completed. If you require assistance assigning multiple phone numbers to flows, let us know in your support request.

   **Important**
   
   If you do not assign the phone number to the flow, calls will not arrive successfully to your Amazon Connect contact center.

2. **Submit a service quota request** at least five days in advance of the mutually agreed date for any changes to your service quotas required to support your use case. For example, you may need to increase the number of concurrent calls per instance, or enable countries for outbound calling.
Step 5: Checklist of activities on your porting date

The action of porting a number can be disruptive: the process involves updating the routing of phone numbers between carriers across a country or Region, including carriers not involved in the actual porting. In rare cases it can take several hours before all routes across all Telecom carriers are fully updated.

Steps you perform to minimize disruption to your phone services

On the mutually agreed port date, perform the following steps:

- Double-check that the activities listed in Step 4 have been completed:
  1. Verify that you have assigned the number being ported into your Amazon Connect instance to the appropriate contact flow.
  2. Verify that any required service quota increases or changes for your Amazon Connect instance were implemented. For example, increase the number of concurrent calls per instance, or enable countries for outbound calling.
- Monitor call traffic from your existing contact center to confirm that incoming traffic has stopped.
- Place test calls to your Amazon Connect instance to verify calls are being routed to the correct flows.
- Ensure agents are logged in to the Contact Control Panel (CCP) and can answer calls as they are received.
- Monitor call traffic to your Amazon Connect instance to confirm that you are receiving the expected levels of traffic.

Steps the Amazon Connect team performs to ensure a smooth transition

1. After the Amazon Connect team receives confirmation that the porting has been completed, we will perform final testing to confirm that the porting was successful and the phone number is receiving calls to Amazon Connect.
2. After we have completed our testing, we will notify you and ask you to verify the successful completion of the porting.
Documentation requirements for porting numbers

The Letter of Authorization (LOA) is an industry standard document type used by carriers to authorize the transfer of a phone number from one carrier to another. In many cases, the LOA is specific to the country or region, carrier, or porting relationship between the losing and winning carriers. If your number can be ported, Amazon Connect support will provide you with an LOA form appropriate for the situation.

For more information, see How to complete an LOA.

Additionally, regulations in some countries require a local business address and specific documentation to use a phone number. For country specific requirements, see Region requirements for ordering and porting phone numbers. If this is required, we will ask for this information to be submitted with the completed LOA.

Common reasons why carriers reject an LOA

There are four common reasons that an LOA may be initially rejected by the losing carrier:

- Unsatisfactory business relationship

  This usually means that you have an unpaid balance or the carrier charges a port away fee. After you pay the bill or fee to your carrier, we will resubmit the port request.

- Name or address mismatch

  The information you submitted on your Letter of Authorization (LOA) is different from what's on file with your carrier in their Customer Service Record (CSR). To fix this, contact your existing carrier to update your CSR information, obtain the correct CSR information, or both. Let us know when they update your information and we will resubmit the port request. Or, send us a new LOA with the correct information as provided by your existing carrier.

- Number cannot be ported

  We will work with all Amazon Connect carriers in a Region to support the porting of your numbers. In some cases, however, specific numbers may not be portable because of regulatory restrictions or carrier limitations. In these situations, consider claiming a new number from Amazon Connect.

- Missing information

  One or more fields have been left blank on the LOA. This may include a missing signature, phone number, address information, or other requested information. Review all LOAs before submitting
them to ensure that you have filled out all requested data. After the LOA is updated with all the required information, we will resubmit the port request.

How to verify flows before numbers are ported

We recommend that you test your call flows before the mutually agreed date and time of porting. If you would like to test your call flows, we recommend that you claim a direct inward dial (DID) or toll-free phone number available within Amazon Connect and assign it to the call flow for testing.

When you are done testing, you can release the number from your instance so you will no longer be charged for it. For instructions, see Release a phone number from Amazon Connect back to inventory.

Until you release the number, you are charged the daily rate associated with claiming a phone number and the per minute rate for telephony minutes used. For more information see the standard pricing for Amazon Connect service usage and associated telephony rates.

After the porting process completes

After you have ported your numbers to Amazon Connect, use the topics in this section to troubleshoot issues, or to release numbers you no longer need after porting.

Contents

- Not receiving calls on the ported number
- Release ported numbers that you no longer need
- Revert to original carrier after porting
- Port phone numbers away from Amazon Connect

Not receiving calls on the ported number

After the scheduled porting window has completed, if you are not receiving phone calls on the ported phone number, update your support ticket. We will troubleshoot with our carrier to verify the porting status and identify the next steps to resolve issue.

Amazon Connect and our carriers make every effort to ensure number porting occurs with minimal downtime and without issues. In most cases, the losing carrier is responsible for initiating the number porting and releasing your number to the winning carrier.
In rare situations, a number routing issue can occur, resulting in calls not arriving to Amazon Connect from the carrier.

**Release ported numbers that you no longer need**

You do not have to keep phone numbers assigned to your Amazon Connect instance.

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.

**To release a phone number**

1. Log in to Amazon Connect admin website with an Admin account or a user account that has **Phone numbers - Release** security profile permission.
2. On the navigation menu, choose **Channels, Phone numbers**. This option appears only if you have the **Phone numbers - View** permission in your security profile.
3. Choose the phone number you want to release, and then choose **Release**. This option appears only if you have the **Phone numbers - Release** permission in your security profile.

If the phone number is associated with a flow, that flow will be deactivated until another number is associated with it.

When customers call the phone number you have released, they will get a message that it is not a working phone number.

**Revert to original carrier after porting**

To complete the porting, the losing and gaining carriers both make configuration changes to pass the phone number ownership. After the porting is complete, the gaining carrier has sole control of the phone number.

To move the phone number again, you must complete a new LOA and any required documentation.

**Port phone numbers away from Amazon Connect**

1. Choose **Account and billing** to go to the pre-populated form in the AWS Support console. You must be signed in to your AWS account to access the form.
2. For **Service**, *Connect (Number Management)* should be selected.

3. For **Category**, *Phone Number Port Out* should be selected.

4. Select the required severity.

5. Choose **Next step: Additional information**

6. On the **Additional information** page:
   
   a. Enter the subject.
   
   b. Under **Description**:
      
      i. Let us know you're porting away.
      
      ii. The name of your Amazon Connect instance and the numbers you are porting away.
      
      iii. The name of your new carrier.

7. Choose **Next step: Solve now or contact us**.

8. On the **Solve now or contact us** page:
   
   - Choose the **Contact us** tab and select your **Preferred contact language** and your preferred contact method.

9. Choose **Submit**.

10. The Amazon Connect team will review your ticket and get back to you.

Here's what happens next:

1. AWS Support contacts you, indicating that you should begin the process with the winning carrier.

2. The winning carrier will request that you provide them with following information:
   
   - Proof of ownership of the numbers you want to port away. Provide them with screenshots of the Amazon Connect instance with the phone numbers you want to port away, and screenshots of your AWS bill.
   
   - Usually the winning carrier will require a LOA (Letter of Authorization) that you need to complete. It's important that you provide the correct contact details from your AWS bill.

3. The winning carrier will send the request to AWS Support.

4. AWS Support will verify that the request from the winning carrier matches the information we have about who owns those numbers. If all details match **exactly**, we will approve the request.
Important

Verifying the authenticity of the winning carrier’s port-out request is critical for the security of your phone number. If the contact details are not correct (for example, there’s a name mismatch), your port-out request may be rejected, causing delays and requiring you to resubmit your request.

5. The winning carrier will complete the port-out request on the date and time that you establish with them. Work with the winning carrier to complete the remainder of the port-out process to ensure a seamless transition.

How to get an Amazon Connect phone number in your current country

To place or receive calls in your Amazon Connect instance, you need to claim a DID or toll-free phone number. If you did not claim a phone number when you created your Amazon Connect instance, follow these steps to claim one now.

Claim a number for your contact center

1. Log in to Amazon Connect admin website with an Admin account, or an account assigned to a security profile that has **Phone numbers - Claim** permissions.
2. On the navigation menu, choose **Channels, Phone numbers**.
3. Choose **Claim a number**. You can choose a toll-free number or a Direct Inward Dialing (DID) number. If you’re in the US, you can specify the area code you want for your number, and only available numbers with that area code will be displayed. When numbers are returned, choose one.
Note

Use the Amazon Connect service quotas increase form for these situations:

- If you select a country or region, but no numbers display, you can request additional numbers for the country or region.
- If you want to request a specific area code or prefix that you don't see listed, we'll try to accommodate your request.

4. Enter a description for the number and, if required, attach it to a contact flow in Flow / IVR.

5. Choose Save.

6. Repeat this process until you have claimed all your required phone numbers.

7. After you claim your numbers, associate them with your flow(s). A flow defines the customer experience with your contact center from start to finish.

How many phone numbers you can claim

There is a service quota for how many phone numbers you can have in each instance. For the default service quota, see Amazon Connect service quotas. If you reach your quota, but want a different phone number, you can release one of your previously claimed numbers. You cannot claim the same phone number after releasing it.

If you need more phone numbers, you can request a service quota increase using the Amazon Connect service quota increase form.

Avoid being blocked from claiming or releasing too many numbers

If you plan to claim and release numbers frequently during a 30 day period, contact us for a service quota increase. Otherwise, it's possible you will be blocked from claiming and releasing any more numbers until 30 days past the oldest number released has expired.

By default you can claim and release up to 200% of your maximum number of active phone numbers during any 30 day period. If you claim and release phone numbers using the UI or API during a rolling 30 day cycle that exceeds 200% of your phone number service level quota, you will be blocked from claiming any more numbers until 30 days past the oldest number released has expired.
For example, if you already have 99 claimed numbers and a service level quota of 99 phone numbers, and in any 30 day period you release 99, claim 99, and then release 99, you will have exceeded the 200% limit. At that point you are blocked from claiming any more numbers until you open an AWS support ticket.

**API instructions for claiming phone numbers**

To claim a phone number programmatically:

1. Use the [SearchAvailablePhoneNumbers](#) API to search for available phone numbers that you can claim to your Amazon Connect instance.

2. Use [ClaimPhoneNumber](#) API to claim the phone number.

   Claiming a number by using the [ClaimPhoneNumber](#) API puts the number in one of the following three states: CLAIMED, IN_PROGRESS, FAILED.

3. Run the [DescribePhoneNumber](#) API to determine the status of your number claiming process.

   - CLAIMED means the previous [ClaimPhoneNumber](#) or [UpdatePhoneNumber](#) operation succeeded.
   - IN_PROGRESS means a [ClaimPhoneNumber](#) or [UpdatePhoneNumber](#) operation is still in progress and has not yet completed. You can call [DescribePhoneNumber](#) at a later time to verify if the previous operation has completed.
   - FAILED indicates that the previous [ClaimPhoneNumber](#) or [UpdatePhoneNumber](#) operation has failed. It will include a message indicating the failure reason. A common reason for a failure may be that the TargetArn value you are claiming or updating a phone number to has reached its limit of total claimed numbers. If you received a FAILED status from a [ClaimPhoneNumber](#) API call, you have one day to retry claiming the phone number before the number is released back to the inventory for other customers to claim.

   **Note**

   You will not be billed for the phone number during the 1-day period if number claiming fails.
"You've reached the limit of Phone Numbers. To increase the limit, contact support."

Even if it's the first time you've claimed a phone number, it's possible to get this error message when you attempt to claim a number. All the issues that cause this error message require help from AWS Support to resolve.

Contact AWS Support and they will provide assistance.

If you have a Basic plan, perform the following steps to contact AWS Support for this issue:

1. In the AWS console, choose AWS Support Center.
2. Choose Create case.
3. Choose Looking for service limit increases?, as shown in the following image.

![AWS Support Center](image)

4. On the Create case page, choose Service limit increase. In the Limit type dropdown box, choose Amazon Connect.
5. Complete the rest of the form, describing the issue and how to contact you. Choose Submit.
6. We'll contact you to help with your request.
Request an SMS-enabled phone number through Amazon Pinpoint SMS

⚠️ Important

Some countries require phone numbers and sender IDs to be registered for use in the country. It can take up to 15 business days to process a registration request after it is submitted. We strongly recommend you begin this process early. For more information about registering, see Registrations.

Using Amazon Pinpoint SMS, you can request new SMS-enabled phone numbers or reuse existing SMS-enabled phone numbers for use in Amazon Connect. You can request short codes, 10-digit long codes (10DLC), and toll-free numbers. These are also known as Origination Identities (OIDs).

For instructions about procuring a number for SMS messaging, see Requesting a phone number in the Amazon Pinpoint SMS User Guide.

Best practices for requesting SMS numbers

- Each type of OID has a different registration process and the leasing costs vary. Review the pricing here: Amazon Pinpoint SMS pricing.

- When deciding what type of phone number to request, we recommend considering your throughput needs. SMS messages are delivered in 140-byte sections known as message parts. Your throughput rate is the number of message parts that you can send each second.

- **1–3 message parts per second**: Use a toll-free number. We recommend using a 10DLC number or short code if your throughput needs will exceed these limits as you expand your use cases. These number types provide plenty of room for growth, but also cost more and currently take longer to obtain than a toll-free number. For more information about requesting a toll-free number in Amazon Pinpoint, see Requesting a phone number.

- **10–75 message parts per second**: Use a 10DLC number. You can also use a short code, which would provide additional room for growth, but would also cost more. For more information, see Requesting dedicated long codes for SMS messaging with Amazon Pinpoint SMS.

- **100 message parts per second or more**: Use a short code. When you create your request in the AWS Support Center Console, specify the throughput rate that you want your short code to support.
By default US short codes support 100 message parts per second, but the throughput rate can be increased beyond that rate for an additional monthly fee. For more information, see Requesting short codes for SMS messaging with Amazon Pinpoint SMS.

- Request at least one of the above OIDs as a TRANSACTIONAL number from Amazon Pinpoint.
- Be sure to provide all of the information requested during the registration process. There are no exceptions to the questions being asked.

**Important**

Providing incomplete or inaccurate information will increase the registration time. Your registration will need to be edited and returned to be reviewed again. Registration for all types of OIDs in the US are managed by a third-party registrar. Amazon does not review applications.

- Toll-free phone number registration requires the least amount of time to procure.
- Review the 10DLC registration process explained in the Amazon Pinpoint SMS User Guide.

### Claim a phone number you already own in another country

Let's say your business is located in Germany. You also have agents in Japan to serve customers who live there, and you need a Japanese phone number for that contact center. To claim a phone number that you already own in another country, use the following steps to create a support case.

To claim a number that you don't already own in another country or Region, see Request numbers, international numbers, or termination points.

1. Go to [Create case](#).
2. Choose [Service limit increase](#).
3. In Limit type select [Amazon Connect](#).
4. In Use case description, provide the address of your business that's located in the other country.
5. In Contact options, choose whether we should contact you by email or phone.
6. Choose [Submit](#).
We'll contact you to help with your request.

**List the phone numbers claimed to your Amazon Connect instance**

You can list the phone numbers claimed to your Amazon Connect instance by using the Amazon Connect console, or by using the `ListPhoneNumberV2` API.

**To list phone numbers by using the Amazon Connect console**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. On the navigation menu, choose Channels, Phone numbers.

   The list of phone numbers claimed to your Amazon Connect instance is displayed.

**Claim phone numbers for Amazon Connect in the Asia Pacific (Tokyo) Region**

To claim a phone number for an Amazon Connect instance you create in the Asia Pacific (Tokyo) Region, open an AWS support case and provide documentation that your business is located in Japan.

⚠️ **Important**

You must provide three pieces of required documentation. For a list of acceptable identification, see [Japan (JP)](https://aws.amazon.com/connect/regions/japan-identification-documentation/) in the Region requirements for ordering and porting phone numbers topic.

You cannot claim numbers for personal use, only for business use.

Amazon Connect supports claiming the following phone numbers for instances created in the Asia Pacific (Tokyo) Region.

- **Direct Inward Dialing (DID) numbers**—DID numbers are also referred to as local numbers.
  - 050 prefix numbers.
  - 03 prefix for numbers in Tokyo. Amazon Connect does not offer phone numbers for other cities in Japan at this time.
- **Toll Free numbers**
• 0120 prefix numbers.
• 0800 prefix numbers.

⚠️ Note
When you claim a toll free phone number for Amazon Connect, there is no corresponding DID number with a 03 prefix also assigned, as with other toll free numbers in Japan. If you need to use a DID number, you can claim one in Amazon Connect.

Request numbers, international numbers, or termination points

⚠️ Important
To purchase and own a phone number, country or region regulations often require:

• A local office address.
• Specific identification documents.

For identification requirements by country, see Region requirements for ordering and porting phone numbers.
In most countries it takes 2-6 weeks for us to fulfill your request. In some cases it can take up to 60 days. If you need a number by a certain date, let us know in your AWS Support case.

⚠️ Note
Amazon does not provide the following:

• Premium rate or higher cost services
• Vanity numbers such as 1-888-555-0000 or an exact number

If you want these services we recommend you contract with specialist providers. For premium rate services you can route calls into Amazon Connect DIDs following local
country regulations. For vanity numbers, after you've purchased them you can move these numbers across to Amazon Connect by porting them.

To request international phone numbers that require documentation, or numbers not available within a specific region, create an AWS Support case. In the support case, you must specify exactly how many numbers you want for each country.

Submit an Amazon Connect support ticket to verify if your phone number can be ported to Amazon Connect.

**Premium support plan**

2. Choose **Create case**.
3. Choose **Technical support**.
4. In **Case details**, do the following:
   a. Choose service as **Connect (Contact Center)**.
   b. Choose category as **Phone Number Requests**.
   c. Choose the required severity.
   d. For **Contact Center Instance ARN**, enter the instance ARN (also called the instance ID). For instructions on how to find your instance ARN, see [Find your Amazon Connect instance ID/ARN](#).
   e. Enter the subject.
   f. Under **Case description**, **Use case description**, include as much information as possible about your request. If you don't know all of these details, you can leave information out.
5. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.
6. Choose **Submit**.
7. The Amazon Connect team will review your ticket and get back to you.

We'll contact you to help with your request.
After your request is approved, the exact number of requested phone numbers appear in your Amazon Connect console for you to claim. You won’t have access to all available numbers in that country.

**Basic support plan**

2. Choose **Create case**.
3. Choose **Service limit increase**.
4. For **Case details, Limit type**, choose **Amazon Connect**.
5. For **Case description, Use case description**, enter the number that you want to request or exactly how many numbers you want for each country. If you need the number by a certain date, include that, too.
6. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.
7. Choose **Submit**.
8. The Amazon Connect team will review your request and get back to you.

We’ll contact you to help with your request.

After your request is approved, the exact number of requested phone numbers appear in your Amazon Connect console for you to claim. You won’t have access to all available numbers in that country.

**Requirements for Custom Termination Points**

In the Asia Pacific (Sydney) Region, you can request Custom Termination Points.

The term "Custom Termination Points" means custom Tier 1 telephony destinations for customer calls to Amazon Connect configured as local phone numbers. In using Custom Termination Points, you understand and agree that you:

1. Have a current toll-free national service that allows you to set Custom Termination Points as a destination for customer phone calls.
2. Cannot port or move Custom Termination Points to a different telephony provider once assigned by Amazon Connect.
3. Will be billed at the standard daily rate for claimed Australian phone numbers and DID inbound usage fees.

4. You are responsible for adding the Custom Termination Points in your existing toll-free national service.

**Move a phone number across instances**

You can move your claimed phone number from one instance or traffic distribution group to another instance or traffic distribution group in the same AWS Region.

Moving a number by using the [UpdatePhoneNumber](#) API puts the number in one of the following three states. You can run the [DescribePhoneNumber](#) API to determine the status of your number moving process.

- **IN_PROGRESS** means a [UpdatePhoneNumber](#) operation is still in progress and has not yet completed. You can call [DescribePhoneNumber](#) to verify if the previous operation has completed.

- **CLAIMED** means the previous [UpdatePhoneNumber](#) operation succeeded and the phone number is not available to be claimed by other customers.

- **FAILED** indicates that the previous [UpdatePhoneNumber](#) operation has failed. It also includes a message that indicates the reason for the failure.

**Release a phone number from Amazon Connect back to inventory**

If you want a different phone number, or have extra numbers that you aren't using, you can release them back to inventory. You can do this using the Amazon Connect console, or programmatically by using the [ReleasePhoneNumber](#) API.

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.
Tip
If you want to close your Amazon Connect account, do these steps for all of your phone numbers. This will ensure you aren’t billed if people erroneously call numbers that you’ve claimed, and initiate your flows. You may also want to delete your instances.

To release a phone number

1. Log in to Amazon Connect admin website with an Admin account or a user account that has Phone numbers - Release security profile permission.
2. On the navigation menu, choose Channels, Phone numbers. This option appears only if you have the Phone numbers - View permission in your security profile.
3. Choose the phone number you want to release, and then choose Release. This option appears only if you have the Phone numbers - Release permission in your security profile.

If the phone number is associated with a flow, that flow will be deactivated until another number is associated with it.

When customers call the phone number you have released, they will get a message that it is not a working phone number.

To use the ReleasePhoneNumber API

- Releasing a number by using the ReleasePhoneNumber API puts the number in a cool down period for 30 days. The phone number cannot be searched for or claimed until after the cool down period ends.

Note
You will not be billed for the phone number during the 30-day cool down period.

Avoid being blocked from claiming or releasing too many numbers

If you plan to claim and release numbers frequently during a 30 day period, contact us for a service quota increase. Otherwise, it’s possible you will be blocked from claiming and releasing any more numbers until 30 days past the oldest number released has expired.
By default you can claim and release up to 200% of your maximum number of active phone numbers during any 30 day period. If you claim and release phone numbers using the UI or API during a rolling 30 day cycle that exceeds 200% of your phone number service level quota, you will be blocked from claiming any more numbers until 30 days past the oldest number released has expired.

For example, if you already have 99 claimed numbers and a service level quota of 99 phone numbers, and in any 30 day period you release 99, claim 99, and then release 99, you will have exceeded the 200% limit. At that point you are blocked from claiming any more numbers until you open an AWS support ticket.

**Third-party numbers**

In some countries you may need to obtain a third-party phone number that is hosted directly by a carrier in that country instead of being hosted by Amazon Connect. The carrier is interconnected with Amazon Connect and provides billing services. In these situations you need to open a ticket to AWS Support to map your AWS account ID and Amazon Connect instance to the phone number.

**To map third-party numbers to your account**

1. If you have an AWS Support account, go to [Support Center](#) and submit a ticket.
   
   Otherwise, open the [AWS Management Console](#) and choose **Support, Create case, Looking for service limit increases.**

2. Add your **Contact Center Instance ARN**.

4. In the Use case description box, add the name of your Partner, and the numbers you want to load and their respective phone number types (DID or toll free).

5. Choose a Contact option and then Submit.

**UIFN service**

A Universal International Freephone number (UIFN) is a unique freephone number that can be used throughout the world. It provides toll-free calling from international locations to your contact center.

Amazon Connect supports UIFN in more than 60 countries that are registered with the International Telecommunications Union, an organization that supports the administration of the UIFN service.

![Note](image)

Amazon Connect allows you to enable UIFNs in as many countries as you need, however, it requires a minimum of 5 countries.

A UIFN is composed of a 3-digit country code for a global service application, such as 800, and an 8-digit Global Subscriber Number (GSN). This results in an 11-digit fixed format.

For example, your UIFN could be +800 12345678, where 12345678 is your number.

Due to the special nature of UIFN, attempting to call a UIFN from Amazon Connect in a "loopback mode" is not supported. UIFNs are designed to be called from end phone configurations in the country's public telephone network.

**How to get a UIFN**

To request a UIFN within a specific AWS Region, create an AWS Support case. In the support case, provide the following information.

- Choose the countries you want to enable from the list of available countries.
- The Amazon Connect instance(s) associated with the new UIFN numbers. Amazon Connect can support routing numbers to multiple Regions, such as Australia to the Asia Pacific (Sydney) Region, United States to a US Region, or if desired to a single global instance.
The required ID verification for your country. Most countries subscribe to standard ID verification requirements for ordering UIFN numbers. However, we recommend checking Region requirements for ordering and porting phone numbers for your country to be sure.

For number portability, after you open a case, Amazon will provide you with Service Provider Change Authorization and Designation of Agency document.

Amazon Connect can route UIFNs to multiple AWS Regions. For example, if a UIFN is enabled for Australia, it can be routed to your Amazon Connect instance that is located in the Asia Pacific (Sydney) Region. If a UIFN is enabled for more countries, each country can be routed to your Amazon Connect instance, which may be in any supported AWS Region.

The following image shows the body of a sample UIFN request submitted to AWS Support. This request is for two UIFNs. The first is for a UIFN that is enabled for Argentina, Brazil, and Colombia, and connected to an Amazon Connect instance in the US West (Oregon) Region. The second request is for a UIFN that is enabled for Japan, Australia, and New Zealand and connected to an Amazon Connect instance located in the Asia Pacific (Singapore) Region.

```
New UIFN number request

arn:aws:connect:us-west-2:your_AWS_accountID:instance/your_instanceARN
Argentina
Brazil
Colombia

arn:aws:connect:ap-southeast-1:your_AWS_accountID:instance/your_instanceARN
Japan
Australia
New Zealand
```

⚠️ Important

Before opening a ticket, be sure to check the National reachability of the country in the following section. Full National reachability means the UIFN reaches all local (in-country) networks. UIFNs in some countries have limited reachability and will only work with specific carriers/networks.
# Countries that support UIFNs

<table>
<thead>
<tr>
<th>Country</th>
<th>How to dial a UIFN and Reachability</th>
<th>How many days it takes a UIFN to be set up</th>
</tr>
</thead>
</table>
| Argentina  | 00-800-XXXX-XXXX  
  National reachability: all fixed networks                                                           | 10-15                                    |
| Australia  | 0011-800-XXXX-XXXX  
  National reachability: full                                                                               | 10-60                                    |
| Austria    | 00-800-XXXX-XXXX  
  National reachability: full                                                                               | 10-15                                    |
| Belgium    | 00-800-XXXX-XXXX  
  National reachability: full                                                                               | 10                                       |
| Brazil     | 0021-800-XXXX-XXXX  
  National reachability: full                                                                               | 20-30                                    |
| Bulgaria   | 00-800-XXXX-XXXX  
  National reachability: full                                                                               | 10-15                                    |
| Canada     | 011-800-XXXX-XXXX  
  National reachability: full                                                                               | 20-30                                    |
| China      | 00-800-XXXX-XXXX  
  National reachability: China telecom fixed and mobile networks                                           | 20-30                                    |
<table>
<thead>
<tr>
<th>Country</th>
<th>How to dial a UIFN and Reachability</th>
<th>How many days it takes a UIFN to be set up</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National reachability: China Unicom fixed network</td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td>1-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Costa Rica</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Croatia</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: all fixed; T-Mobile network</td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full, including Monaco</td>
<td></td>
</tr>
<tr>
<td>French Guiana</td>
<td>00-800-XXXX-XXXX</td>
<td>15-25</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>How to dial a UIFN and Reachability</td>
<td>How many days it takes a UIFN to be set up</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Germany</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: all fixed; Cosmotel mobile network</td>
<td></td>
</tr>
<tr>
<td>Guadeloupe</td>
<td>00-800-XXXX-XXXX</td>
<td>15-25</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td>006-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Iceland</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: all fixed; Iceland Telecom, IMC, Vodafone mobile networks.</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td>Italy</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: all fixed networks, including Vatican and San Marino</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>How to dial a UIFN and Reachability</td>
<td>How many days it takes a UIFN to be set up</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Japan</td>
<td>010-800-XXXX-XXXX</td>
<td>20-50</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td>Lithuania</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Macao</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Macedonia</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: MakTel fixed, T-Mobile network</td>
<td></td>
</tr>
<tr>
<td>Malta</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: MELITA, OZONE, SIS, VANILLA, VODAFONE fixed; Melita, Redtouch Fone, Vodafone, YOM mobile networks. Note that coverage includes Malta, Gozo, and Comino Island.</td>
<td></td>
</tr>
<tr>
<td>Martinique</td>
<td>00-800-XXXX-XXXX</td>
<td>40-60</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>How to dial a UIFN and Reachability</td>
<td>How many days it takes a UIFN to be set up</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Mayotte</td>
<td>00-800-XXXX-XXXX</td>
<td>15-25</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Monaco</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Peru</td>
<td>00-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>Mobile reachability: Telefónica del Peru F&amp;M network guaranteed only. Other networks are not guaranteed.</td>
<td></td>
</tr>
<tr>
<td>Philippines</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: all fixed networks</td>
<td></td>
</tr>
<tr>
<td>Portugal</td>
<td>00-800-XXXX-XXXX</td>
<td>15-25</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>How to dial a UIFN and Reachability</td>
<td>How many days it takes a UIFN to be set up</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Reunion</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Romania</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: Orange fixed and mobile network, Rodasy fixed and mobile network, Romtelekom fixed and mobile network, Cosmote mobile network</td>
<td></td>
</tr>
<tr>
<td>Saint Pierre And Miquelon</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>001 800 XXXX XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td></td>
<td>The subscriber's mobile must subscribe to 001 dialing routes with their service subscriber</td>
<td></td>
</tr>
<tr>
<td>Slovakia</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Slovenia</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td>00-800-XXXX-XXXX</td>
<td>10-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>South Korea</td>
<td>002-800-XXXX-XXXX</td>
<td>20-30</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td><strong>How to dial a UIFN and Reachability</strong></td>
<td><strong>How many days it takes a UIFN to be set up</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Spain</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Concurrent calls: 100 consecutive calls</td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td>001-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>00-800-XXXX-XXXX</td>
<td>15-30</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td>00-800-XXXX-XXXX</td>
<td>10-15</td>
</tr>
<tr>
<td></td>
<td>National reachability: full</td>
<td></td>
</tr>
</tbody>
</table>

**Region requirements for ordering and porting phone numbers**

Country or region regulations often require a local office address and specific identification documents to purchase and own a phone number. The address that you provide can be the business or personal address where the phone numbers are used.

For a list of the telephony capabilities that Amazon Connect provides, see the [Amazon Connect Telecoms Country Coverage Guide](#).

Following is a list of ID Requirements by country or region. When you [request an international number](#), we'll work with you to submit your documents.
Important

- Addresses that can be claimed without presence, such as PO Box addresses, are not valid in any country.
- After your numbers are ordered or ported, the exact number of requested phone numbers appear on the Manage Phone numbers page in the Amazon Connect admin website for you to manage. You won't have access to all available numbers in that country.

Anguilla (AI)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>
Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

Antigua and Barbuda (AG)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 268</td>
<td>Yes</td>
<td>File orders in writing. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
</tbody>
</table>

Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

Argentina (AR)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +54 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>EIFN</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
</tbody>
</table>
## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 2AM-4AM or 10AM-12PM or 3PM-5PM UTC-3 Buenos Aires time</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Argentinian AFIP (Federal Tax Agency) extract, as proof of CUIT (Clave Única de Identificación Tributaria - Unique Tax Payer ID)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Scanned copy of the Power of Attorney assigning the signatory sufficient attributes that allow them to request the portability, or Company Statute where the signatory appears with such attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Scanned copy of the DNI (National Identity Card) of the signatory with power of attorney</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Australia (AU)

For UIFN numbers, supports standard [Regions and requirements](#).

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address, a contact name, and phone number. An address in Australia is required</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +61 1300, +61 1800</td>
<td>No</td>
<td>Your business address, a contact name, and phone number. A global address is acceptable.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focused on:</td>
<td>Monday-Friday 8 AM -12 PM AEST</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>(Seoul)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Tokyo)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Austria (AT)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Proof of telecom services at your address, which must match the city code requested. Valid forms of proof (must be issued in the past 6 months):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Invoice from a network operator for another phone number, at your address</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +43 720</td>
<td>Yes</td>
<td>• Invoice from an internet services provider for internet access with fix IP address, at your address</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +43 800</td>
<td>Yes</td>
<td>Proof of telecom services at your address, which must be within the country. Valid forms of proof (must be issued in the past 6 months): • Invoice from a network operator for another phone number, at your address • Invoice from an internet services provider for internet access with fix IP address, at your address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Your business name, address, and a copy of the business registration (global). A global address is acceptable.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focused on:</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Belgium (BE)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +32 46</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +32 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focused on:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>3. Mandatory to provide service address for the numbers</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Bahamas (BS)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 242</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
</tbody>
</table>

Region requirements for ordering and porting phone numbers
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barbados (BB)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 246</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

### Barbados (BB)

**For ordering phone numbers**

- Barbados (BB)

  **Supported Regions**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 246</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Use the form that is provided to you when you make the request. Provide the following information:
  - Your name and address
  - A description of the service for which the number(s) will be used

- A global address is acceptable.
Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

Bolivia (BO)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>National prefixes: +591 50</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Local telephone numbers: +599 7</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
</tbody>
</table>

Number portability

Porting is not supported.

Bonaire (BQ)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +599 7</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A description of the service for which the number(s) will be used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>

**Number portability**

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

**Brazil (BR)**

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>How to access</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes. Local Brazilian presence is required.</td>
<td>To obtain numbers in Brazil:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. An AWS Support representative will contact you. They will put you in contact with our local telephony provider to provide you with an in Country-Specific Agreement.</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>How to access</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>After you have your numbers from our carrier, perform the steps explained in <a href="#">Third-party numbers</a> to add your numbers to your Amazon Connect instance.</td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>How to access</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes. Local Brazilian presence is required.</td>
<td>• If you currently have local numbers in Amazon Connect: 1. Coordinate with the telephony provider that we have contracted with for your number porting. 2. Open an AWS Support ticket to have your ported numbers added to your Amazon Connect instance.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Region requirements for ordering and porting phone numbers

304
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>How to access</th>
</tr>
</thead>
</table>

- If you are in the process of porting numbers and do not yet have local numbers in Brazil associated with your Amazon Connect instance, follow the steps outlined above for ordering numbers. This includes opening a ticket with AWS Support to initiate the process.
Brunei (BN)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Toll-free prefixes:</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
</tbody>
</table>

Number portability

Porting is not supported.

Canada (CA)

For UIFN numbers, supports standard [Regions and requirements](#). For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
## Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 7 AM to 5 PM CST</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS GovCloud (US-West)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Chile (CL)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes:</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia)   | Monday-Friday 9 PM to 3 AM PST | 1. Last invoice  
                        |                                                           | 2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
                        |                                                           | 3. Copy of legal representative's photo ID  
                        |                                                           | 4. Copy of local business registration |
| US West (Oregon)        |                            |                                                          |
# China (CN)

## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Colombia (CO)**

For UIFN numbers, supports standard [Regions and requirements](#).
For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +57 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Costa Rica (CR)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Businesses must provide a copy of business registration containing a proof of address as well as an ID of an authorised representative. Valid proofs of address include: third-party issued bank statements,</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>utility bills (all issued in the previous 6 months); government documents (issued in the previous year); the proof of ID is a copy of the national identity ID or passport of an authorized representative.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The business address must be inside of Costa Rica.</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +506 800</td>
<td>Yes</td>
<td>Businesses must provide a copy of business registration containing a proof of address as well as an ID of an authorised representative. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year); the proof of ID is a copy of the national identity ID or passport of an authorized representative. The business address must be inside of Costa Rica.</td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Croatia (HR)

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your residence or business address. Both must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Toll-free prefixes: + 385 800</td>
<td>Yes</td>
<td>Your business name and address. A global address is acceptable.</td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice  2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it. 3. Copy of Court Registration 4. Copy of legal representative's photo ID 5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Curaçao (CW)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +599 9</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>

Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).
## Cyprus (CY)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Toll-free prefixes: + 357 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice&lt;br&gt;2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it. &lt;br&gt;3. Copy of <strong>Certificate of Directors and Secretary of the Company</strong>&lt;br&gt;4. Copy of <strong>Certificate of Incorporation</strong>&lt;br&gt;5. Copy of legal representative's photo ID</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Czech Republic (CZ)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your residence or business address. Both must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +420 800</td>
<td>Yes</td>
<td>Your business name and address. A global address is acceptable.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 3 PM to 4 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required per Type of Number as listed in the previous table for ordering numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Denmark (DK)

For UIFN numbers, supports standard [Regions and requirements](#).

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business name, address, and service description. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +45 9x</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +45 808</td>
<td>Yes</td>
<td>Your business name, address, and service description. A global address is acceptable.</td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Focused on:       | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
| US East (N. Virginia) |                      | 2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
| US West (Oregon)  |                      | 3. Documents required per Type of Number as listed in the previous table for ordering numbers  
| Europe (Frankfurt) |                      |  
| Europe (London)   |                      |  |
Dominican Republic (DOM)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +1 8xx</td>
<td>No</td>
<td>NA</td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10:00PM to 04:00AM PST</td>
<td>1. Letter of Authorization (LOA) signed: When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Only Local Address accepted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Copy of the ID or passport of an authorized representative who signs the LOA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Copy of Local Commercial Registry Number known as RNC / &quot;Número de Registro Mercantil&quot;.</td>
</tr>
</tbody>
</table>
## Ecuador (ECU)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +593-180000XXXX</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## El Salvador (SV)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Businesses must provide their name, address, and RUC/ TaxID number, along with a copy of the business registration and a proof of address.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>Valid proofs of address include: third-party issued bank statements,</td>
</tr>
</tbody>
</table>

Region requirements for ordering and porting phone numbers
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>utility bills (all issued in the previous 6 months); government documents (issued in the previous year). A local address is required.</td>
</tr>
</tbody>
</table>

Toll-free prefixes:

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>Businesses must provide a copy of business registration and a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year).</th>
</tr>
</thead>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 03:00AM to 05:00AM CST</td>
<td>1. Letter of Authorization (LOA) Portability Form. When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Monday-Friday 03:00AM to 05:00AM CST</td>
<td>1. Letter of Authorization (LOA) Portability Form. When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
</tbody>
</table>
Supported Regions | Portability windows | Required Documents
--- | --- | ---

Estonia (EE)

For ordering phone numbers

For UIFN numbers, supports standard [Regions and requirements](#).

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Toll-free prefixes: +372 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes: +372</td>
<td>Yes</td>
<td>Your business address. A copy of the ID/business registration. A global address is acceptable.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Europe (Frankfurt) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. LOA template has to include a local address.  
4. If this is a company, a business number is required. |
| Europe (London) | | |

Finland (FI)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your residence or business address. Both must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +358 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>National prefixes: +358 75</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**France (FR)**

For UIFN numbers, supports standard Regions and requirements.

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers and NPV number:</td>
<td>Yes</td>
<td>An address in France is required.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>You must provide a copy of the business registration (KBIS or INSEE extract issued in the past 3 months), listing the provided address in France as main business address.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes: +33 9</td>
<td>Yes</td>
<td>National numbers are temporarily unavailable due to industry impact of Jan 1, 2023 regulatory changes in France.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +33 801</td>
<td>Yes</td>
<td>Toll-free numbers are temporarily unavailable due to industry impact of Jan 1, 2023 regulatory changes in France.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of Number</th>
<th>Prefixes</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPV numbers:</td>
<td>+33 162, 163, 270, 271, 377, 378, 424,425, 568, 569, 948, 949</td>
<td>Amazon Connect does not support ordering or porting of numbers in these ranges.</td>
</tr>
</tbody>
</table>
### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>EU (Frankfurt)</td>
<td></td>
<td>3. Documents required per Type of Number as listed in the previous table for ordering numbers.</td>
</tr>
<tr>
<td>EU (London)</td>
<td></td>
<td>4. It is mandatory to provide RIO code from the losing carrier, or at least the SIRET (if you're a business customers only). You can obtain the SIRET by contacting your existing telecom carrier.</td>
</tr>
</tbody>
</table>

### French Guiana (GF)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Georgia (GE)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>National prefixes: +995 70</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Local telephone numbers: (Tbilisi)</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone as the number. You must provide proof of the address.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Germany (DE)**

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Local address in Germany is required. The address dictates where the geographic number must be sited. Businesses must provide a copy of the business registration document (issued in the past 6 months) as proof of address.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes: +49 32</td>
<td>Yes</td>
<td>An address in Germany is required. Businesses must provide a copy of the business registration document (issued in the past 6 months) as proof of address.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +49 800</td>
<td>Yes</td>
<td>Your business address outside of Germany. You</td>
</tr>
</tbody>
</table>
**Supported Regions** | **Type of Number** | **Are there ID requirements?** | **Acceptable Identification**
---|---|---|---

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. For business ports, end user stamp is mandatory on the LOA.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. If the number to be ported is an extended line, the main line must be ported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

**Greece (GR)**

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +30 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Company registration certificate</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. Copy of LOA signatory's photo ID/Passport</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>
## Guatemala (GT)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes:</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

Porting is not supported.

## Guadeloupe (GP)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Region requirements for ordering and porting phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Honduras (HN)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>National DID:</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +504 800</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

Porting is not supported.

**Hong Kong (HK)**

For UIFN numbers, supports standard [Regions and requirements](#).
For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your address and proof of address.</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +852 58</td>
<td>Yes</td>
<td>A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Toll-free prefixes: +852 800</td>
<td>Yes</td>
<td>Your business address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>N/A</td>
<td>1. Last invoice.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers.</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hungary (HU)

For UIFN numbers, supports standard Regions and requirements.

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone. You must provide a copy of the business registration document (issued in the past 6 months) as proof of address. A copy of the ID or passport of an authorized representative is also required.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Toll-free prefixes: +36 800 No

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Europe (Frankfurt) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice: must be within the last 6 months  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with |
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>a country-specific LOA template and explain how to complete it. 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

**Iceland (IS)**

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Toll-free prefixes:</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

Porting is not supported.

**Indonesia (ID)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile prefixes: +62 855</td>
<td>Yes</td>
<td>Proof of business address, a copy of the ID or passport of an authorized representative, and the business registration. You must also provide a description of how you plan to use the numbers.</td>
</tr>
<tr>
<td>Toll-free prefixes: +62 800</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Ireland (IE)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Toll-free prefixes: +353 1800</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. It is mandatory to provide the main telephone number on the account.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. It is mandatory to provide a Wholesale Account number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Type of the line mandatory on the LOA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>
## Israel (IL)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Italy (IT)**

For UIFN numbers, supports standard [Regions and requirements](#).  

---

Region requirements for ordering and porting phone numbers
## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business name, address, and VAT number. You must provide proof of the address along with a copy of the business registration (extracted within the last 6 months).</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td>You must provide the following details of an authorized representative: name and address, birth location and data, and nationality and tax code. Also provide proof of the authorized representative's identity, which can be a copy of an ID or passport. The name of the representative must appear on the business registration. A local address in Italy is required.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toll-free prefixes: +39 800</td>
<td>Yes</td>
<td>Your business name, address, and VAT number.</td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You must provide the following details of an authorized representative: name and address, birth location and data, and nationality and tax code. Also provide proof of the authorized representative's identity, which can be a copy of an ID or passport. A global address is acceptable.</td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Migration code of the requested number is mandatory. Obtain this code from the losing carrier.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>
### Jamaica (JM)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Local telephone numbers: | Yes | An order form is required. Use the form that is provided to you when you make the request. Provide the following information:  
- Your name and address  
- A description of the service for which the number(s) will be used |
| US West (Oregon) | | | A global address is acceptable. |

#### Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

### Japan (JP)

For UIFN numbers, supports standard [Regions and requirements](#).
## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Businesses must provide 3 pieces of documentation:</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td>• <strong>Company registration documents</strong> (must be issued in the past 6 months). These documents must show:</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td>• The business address is in the city corresponding to the requested area code of the number.</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td>• The authorized representative of the business.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>A copy of the personal ID or passport of the business's authorized representative.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The person must be registered on the Company Registration Documents. Valid personal ID can be</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>government-issued IDs or passports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>Proof of address for the business</strong> (must be issued in the past 6 months).</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>months). Valid proofs of address include: third-party issued bank statements, public utility bills; government documents; or IDs listing the submitted address, such as government-issued IDs, passports, and business registration. Copies of these documents should be made into a single ZIP file.</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +81 120, +81 800</td>
<td>Yes</td>
<td>Businesses must provide the following documentation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>Company registration documents</strong> (must be issued in the past 6 months). These documents must show:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The business address. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The authorized representative of the business.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>A copy of the personal ID or passport of the business's authorized representative.</strong> The person must be registered on the Company Registration Documents. Valid personal ID can be government-issued IDs and passports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Copies of these documents should be made into a single ZIP file.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Asia Pacific (Tokyo) | | 1. Last invoice  
| | | 2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
| | | 3. Documents required per Type of Number as listed in the previous table for ordering numbers  
| | | Submit an AWS Support ticket to verify the portability of your number(s). |

Latvia (LV)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Toll-free prefixes: +371 80</td>
<td>Yes</td>
<td>Businesses must provide a copy of the business registration, along with proof of address within Latvia (issued in the past 6 months).</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td>Valid forms of proof:</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| National prefixes: +371 6 | Yes | - Business Registration  
- Third-party issued bank statement  
- Public utility bill showing regular use  
- Lease Agreement  
- Government documents |

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (London)</td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it. 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

### Lithuania (LT)

For UIFN numbers, supports standard [Regions and requirements](#).

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Toll-free prefixes: +370 800</td>
<td>Yes</td>
<td>Your business address in the country.</td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. VAT number and local address is needed on the LOA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

**Luxembourg (LU)**

For UIFN numbers, supports standard Regions and requirements.

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers: +352 27</td>
<td>Yes</td>
<td>Your residence or business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes:</td>
<td>Yes</td>
<td>An address in Luxembourg is required. Businesses must provide a copy of the business registration.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +352 800</td>
<td>Yes</td>
<td>Your business name and address. A global address is acceptable.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Europe (Frankfurt) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. You must provide the account number from the Main Losing Carrier to which the requested DID is assigned.  
4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers |
| Europe (London)    |                     |                    |

Macao (MO)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Macedonia (MK)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Malaysia (MY)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers</td>
<td>Yes</td>
<td>1. Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td>2. Business Registration Documentation. Numbers can only be assigned to global companies, that are not owned by a Malaysian entity, and that have a branch or local office established in Malaysia, with proof of registration in the country.</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malta (MT)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description.</td>
</tr>
</tbody>
</table>

#### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Malta (MT)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Martinique (MQ)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Mayotte (YT)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Mexico (MX)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +52 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 10 AM to 12 PM CET or 2 PM to 4 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with |
| US West (Oregon) | | |

Region requirements for ordering and porting phone numbers
Supported Regions | Portability windows | Required Documents
--- | --- | ---

- Monaco (MC)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New Zealand (NZ)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Toll-free prefixes: +64 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Monday-Friday 7 AM to 11 AM NZST</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td>2. Letter of Authorization (LOA):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td>3. Wholesale account number of the phone number from the current carrier.</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Netherlands (NL)

For UIFN numbers, supports standard [Regions and requirements](#).

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
</tbody>
</table>
| US West (Oregon)        | Toll-free prefixes: +31 800     | Yes                         | An order form is required. Use the form that is provided to you when you make the request. Provide the following information:  
  - Your name and address.  
  - A description of the service for which the number will be used.  
  A global address is acceptable.  
  Estimated lead time from order to activation is 6 weeks. |
| Canada (Central)        | National prefixes: +31 85       | Yes                         | Your business address in the country.                        |
| Europe (Frankfurt)      |                                 |                             |                                                              |
| Europe (London)         |                                 |                             |                                                              |
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Nicaragua (NI)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

Porting is not supported.
## Norway (NO)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address in Norway, street code, municipality code, and company organization number.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +47 800</td>
<td>Yes</td>
<td>Your business address in Norway, street code, municipality code, and company organization number. Norwegian business registration as proof of address.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>National prefixes: +47 81</td>
<td>Yes</td>
<td>Your business address in Norway, street code, municipality code, and company organization number. Norwegian business registration as proof of address.</td>
</tr>
</tbody>
</table>
Numbers are available to businesses only, not individuals. The DID type is Landline, instead of Geographic. This is because all formerly geographic numbers are now classified as landline, and do not have a geographic zone.

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Panama (PA)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +507 800</td>
<td>Yes</td>
<td>Your business address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You can have a maximum of 5 Panama toll-free numbers per business name.</td>
</tr>
</tbody>
</table>
## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 12 AM to 2 AM PST</td>
<td>For porting local numbers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Last invoice and proof of payment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Letter of Authorization (LOA):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you request porting services, we will provide you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with a country-specific LOA template and explain how</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to complete it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Copy of legal representative's photo ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Copy of local business registration</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>For porting toll-free numbers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Transfer Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Proof of contract termination with the current</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provider, with a defined disconnection date within at</td>
</tr>
<tr>
<td></td>
<td></td>
<td>least 14 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Documents required for the Type of Number, as listed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in the previous table for ordering phone numbers.</td>
</tr>
</tbody>
</table>

### Peru (PE)

For UIFN numbers, supports standard [Regions and requirements](#).
## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +51 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 10 PM to 4 AM PST | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. Copy of legal representative's photo ID  
4. Copy of local business registration |
| US West (Oregon) | | |

## Philippines (PH)

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Poland (PL)

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address and a copy of a business registration.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Mobile prefixes: +48 73</td>
<td>Yes</td>
<td>A global address is acceptable.</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td>Your business name, address and registration</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toll-free prefixes: +48 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

#### Number portability

Number portability is not available for toll-free numbers.

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 12 AM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Portugal (PT)

For UIFN numbers, supports standard [Regions and requirements](#).
## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>National prefixes: +351 30</td>
<td>Yes</td>
<td>Your business address in Portugal. You must also submit the required proof of Telecom services being provided at the address.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +351 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. Copy of legal representative's photo ID  
4. Documents required per Type of Number as listed in the previous table for ordering numbers |
| US West (Oregon) |  |  |
| Europe (Frankfurt) |  |  |
| Europe (London) |  |  |
Puerto Rico (PR)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 787, +1 939</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +1 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM PST</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
</tbody>
</table>

Reunion (RE)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Romania (RO)**

For UIFN numbers, supports standard [Regions and requirements](#).  

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your address and proof of address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes: +40 376</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM PST</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

Saba (BQ)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +599 4</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
</tbody>
</table>
### Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

### Saint Pierre and Miquelon (PM)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A global address is acceptable.
## Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Region requirements for ordering and porting phone numbers 383
**Supported Regions** | **Portability windows** | **Required Documents**
--- | --- | ---
Europe (Frankfurt) |  |  
Europe (London) |  |  

**Serbia (RS)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Toll-free prefixes:**

<table>
<thead>
<tr>
<th></th>
<th>No</th>
</tr>
</thead>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Saint Lucia (LC)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Local telephone numbers: | Yes | An order form is required. Use the form that is provided to you when you make the request. Provide the following information:  
• Your name and address  
• A description of the service for which the number(s) will be used.  
A global address is acceptable. |
| US West (Oregon)  |                                |                            |                                                                                           |

### Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

## Saint Martin (MF)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 758</td>
<td>Yes</td>
<td>An order form is required. Use the form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td>that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>

**Number portability**

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

**Singapore (SG)**

For UIFN numbers, supports standard Regions and requirements.

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>National prefixes: +65 31 and +65 6</td>
<td>Yes</td>
<td>Address required in country.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td>Documents required for company: Company registration documents</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Toll-free prefixes: +65 800</td>
<td>Yes</td>
<td>Your business address. A global address is acceptable.</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

Number portability is not available for toll-free numbers.

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Asia Pacific (Singapore) | NA | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. List of Port in Numbers |

Porting-out is only possible for contiguous number blocks of 10 numbers (...0 to ...9) due to market practice.

### Sint Eustatius (BQ)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +599 3</td>
<td>Yes</td>
<td>An order form is required. Use the form</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| US West (Oregon) | | | that is provided to you when you make the request. Provide the following information:  
- Your name and address  
- A description of the service for which the number(s) will be used |
| | | | A global address is acceptable. |

### Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

### Sint Maarten (SX)

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Region</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Local telephone numbers: +1 721 | Yes | An order form is required. Use the form that is provided to you when you make the request. Provide the following information:  
- Your name and address |
| US West (Oregon) | | | |

---

Region requirements for ordering and porting phone numbers
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Toll-free prefixes: +421 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

**Slovakia (SK)**

For UIFN numbers, supports standard [Regions and requirements](#).  

**For ordering phone numbers**

- A description of the service for which the number(s) will be used
- A global address is acceptable.
### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers |
| US West (Oregon) | | |
| Europe (Frankfurt) | | |
| Europe (London) | | |

### Slovenia (SI)

For UIFN numbers, supports standard [Regions and requirements](#).

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +386 80</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +386 82</td>
<td>Yes</td>
<td>An address in Slovenia is required.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe (Frankfurt)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ordering phone numbers</td>
</tr>
</tbody>
</table>

South Africa (ZA)

For UIFN numbers, supports standard [Regions and requirements](#).

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td>Local numbers:</td>
<td>Yes</td>
<td>Your business address in South Africa, in the relevant geographic zone, along with your Tax ID.</td>
</tr>
<tr>
<td></td>
<td>Mobile numbers:</td>
<td>Yes</td>
<td>Your business address in South Africa and proof of address such as one of the following documents:</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Excerpt from the commercial register showing the South Africa address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Utility bill</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Tax notice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rent receipt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Title deed</td>
</tr>
</tbody>
</table>

Toll-free prefixes: Yes

Your business address in South Africa and a letter of intent (LOI).

You can have a maximum of 9 South Africa toll-free numbers per letter of intent.

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| Africa (Cape Town)      | N/A                 | 1. Last invoice.  
                          |                                    | 2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
                          |                                    | 3. Documents required for the Type of Number, as listed in the |
### South Korea (KR)

**Note**

Ordering and porting numbers in South Korea takes longer than most other countries because of extra steps related to Regulator review, and because the many of the steps must be performed in Korean. For more information about ordering and porting numbers in South Korea, see [Things to know about South Korean numbers, regulations, and porting](#).

For UIFN numbers, supports standard [Regions and requirements](#).

#### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>VoIP prefixes numbers: +82 70</td>
<td>Yes</td>
<td>Local customers should provide a copy of their <strong>business (tax office) registration certificate</strong>, which is issued by local tax authorities and shows the company's registered address. Submit an AWS Support ticket to verify the documents for new number(s) ordering.</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                   | Representative numbers: +82 15, +82 16             | Yes                        | Representative number order form is required. Use the form that is provided to you when you make the request. Along with this form, the following documents are required:  
  - Local customers should provide a copy of their **business (tax office) registration certificate**, which is issued by local tax authorities and shows the company's registered address.  
  Submit an AWS Support ticket to verify the documents for new number(s) ordering. |
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Toll-free prefixes: +82 308</td>
<td>Yes</td>
<td>Your business address in South Korea. Local customers should provide a copy of their <strong>business (tax office) registration certificate</strong>, which is issued by local tax authorities and shows the company's registered address. Submit an AWS Support ticket to verify the documents for new number(s) ordering. Submit an AWS Support ticket to order a new number.</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographic Prefixes: +82 2</td>
<td>Yes</td>
<td>Same as for VOIP numbers, but the provided business registration document should reference a physical location associated with +822 (Seoul) zone. Local numbers are limited per customer due to minimum of 6 months of physical installation of number. If you require a large number of DIDs, order and port these directly to Amazon Connect.</td>
<td></td>
</tr>
</tbody>
</table>

### Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of number</th>
<th>Portability windows</th>
<th>Required documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Geographic Prefixes: +82 2 (any +82 number other than +821, +825, +827, +82308)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>New SIP Order Form and SIP Port Form for the existing number(s). Use the forms that are provided to you when you make the request. Documents must be signed by a company employee whose month</td>
</tr>
</tbody>
</table>

Region requirements for ordering and porting phone numbers
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of number</th>
<th>Portability windows</th>
<th>Required documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>and year of birth are noted, and the company stamp must be applied. Along with these forms the following documents are required:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Korean Business Certificate within 6 months. The certificate must match the geographic zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Personal ID for person signing the form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Certificate of Seal Impression</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Submit an AWS Support ticket to verify the portability of your number(s).</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of number</td>
<td>Portability windows</td>
<td>Required documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                   | National Prefixes: +82 50 | Monday-Friday 10 AM to 12 PM CET | New SIP Order Form and SIP Port Form for the existing number(s). Use the forms that are provided to you when you make the request. Documents must be signed by a company employee whose month and year of birth are noted, and the company stamp must be applied. Along with these forms the following documents are required:  
1. Korean Business Certificate within 6 months. The certificate must match the geographic zone  
2. Personal ID for person signing the form  
3. Certificate of Seal Impression  
Submit an AWS Support ticket to verify the portability of your number(s). |
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of number</th>
<th>Portability windows</th>
<th>Required documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Representative numbers: +82 15, +82 16</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>RN/TFN change form is required. Use the form that is provided to you when you make the request. Along with this form the following documents are required: 1. Copy of the company certified registration within 6 months Submit an AWS Support ticket to verify the portability of your number(s).</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +82 308</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>RN/TFN change form required. Use the form that is provided to you when you make the request. Along with this form the following documents are required: 1. Copy of the company certified registration within 6 months Submit an AWS Support ticket to verify the documents for new number(s) ordering.</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of number</td>
<td>Portability windows</td>
<td>Required documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                   | VoIP prefixes numbers: +82 70 | Monday-Friday 10 AM to 12 PM CET | Effectively, callforward to another +8270 is possible. New SIP Order Form and SIP Port Form for the existing number(s). Use the forms that are provided to you when you make the request. Documents must be signed by a company employee whose month and year of birth are noted, and the company stamp must be applied. Along with these forms the following documents are required: 1. Korean Business Certificate within 6 months. The certificate must match the geographic zone. 2. Personal ID for person signing the form. 3. Certificate of Seal Impression Submit an AWS Support ticket to verify the
<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of number</th>
<th>Portability windows</th>
<th>Required documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>portability of your number(s).</td>
<td></td>
</tr>
</tbody>
</table>

**Spain (ES)**

For UIFN numbers, supports standard Regions and requirements.

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone as the phone number. A copy of the ID/business registration and a proof of address.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Toll-free prefixes: +34 900</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td>National prefixes: +34 902</td>
<td>Yes</td>
<td>An address in Spain is required. A copy of the ID/business registration and a proof of address.</td>
</tr>
</tbody>
</table>
Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. CIF/NIF (VAT number)</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
</tbody>
</table>

Sweden (SE)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address in Sweden.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Mobile prefixes: +46 766</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +46 20</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>National prefixes: +46 77 and +46 10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

Number portability is not available for +46 77 numbers.

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 10 AM to 12 PM CET | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.  
3. Your tax number has to be provided. A Swedish organization number usually contains 12 digits, starting with 16 if it is from a company, or 19 or 20 if it's personal.  
4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers |
| US West (Oregon) | | |
| Europe (Frankfurt) | | |
| Europe (London) | | |

**Switzerland (CH)**

For UIFN numbers, supports standard [Regions and requirements](#).
For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address in the country. A copy of the ID/business registration and a proof of address.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Toll-free prefixes: +41 800</td>
<td>Yes</td>
<td>Your business address and a copy of business registration. A global address is acceptable.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td>3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td>4. Proof of address</td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taiwan (TW)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Taiwan (TW)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Region</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Thailand (TH)

For UIFN numbers, supports standard [Regions and requirements](#).

## For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td><strong>For business address inside Thailand:</strong> Business must provide a copy of the ID of a company authorized representative and company certificate.</td>
<td>International caller ID is not guaranteed.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td><strong>For business address outside of Thailand:</strong> Proof of business address and proof of ID, such as the business registration. Also, a copy of the ID or passport of an authorized representative.</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toll-free prefixes: +66 1800</td>
<td>Yes</td>
<td>Proof of business address and proof of ID, such as the business registration. Also, a copy of the ID or passport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
<td>Restrictions</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>--------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Trinidad and Tobago (TT)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers: +1 868</td>
<td>Yes</td>
<td>An order form is required. Use the form that is provided to you when you make the request. Provide the following information:</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Local telephone numbers: +1 868</td>
<td>Yes</td>
<td>• Your name and address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A description of the service for which the number(s) will be used</td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------</td>
<td>----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Turks and Caicos (TC)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

**Turks and Caicos (TC)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Local telephone numbers: +1 649 | Yes                         | An order form is required. Use the form that is provided to you when you make the request. Provide the following information:  
  
  - Your name and address  
  - A description of the service for which the number(s) will be used |
| US West (Oregon)   |                                      |                            | A global address is acceptable. |
Number portability

Porting of specific number ranges is supported. Create an AWS Support ticket to verify the portability of your number(s).

Uganda (UG)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be inside of Uganda.</td>
</tr>
</tbody>
</table>

Toll-free prefixes | No |  |

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
United Kingdom (GB)

For UIFN numbers, supports standard [Regions and requirements](#).

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Mobile prefixes: +44</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Toll-free prefixes: +44 800, +44 808</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>National prefixes:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Monday-Friday 10 AM to 12 PM CET</td>
<td>1. Last invoice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Letter of Authorization (LOA): When you request porting services, we will provide you with a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**United States (US)**

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada (Central)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
</table>
| US East (N. Virginia) | Monday-Friday 7 AM to 5PM CST | 1. Last invoice  
2. Letter of Authorization (LOA): When you request porting services, we will provide you with |
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td>a country-specific LOA template and explain how to complete it.</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Uruguay (UY)

For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Portability windows</td>
<td>Required Documents</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vietnam (VN)**

**For ordering phone numbers**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Toll-free prefixes:</td>
<td>yes</td>
<td>Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents</td>
</tr>
</tbody>
</table>
## Coverage Limitations

- **Local**: All major networks except minority three networks FPT, CMC and Gtel.
- **TFN**: National reachability only from: VNPT fixed network, Vinaphone Mobile, and SPT network.

## Number portability

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not supported</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## UIFN requirements

### For ordering phone numbers

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Type of Number</th>
<th>Are there ID requirements?</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>UIFN</td>
<td>Yes</td>
<td>Your business name, address and service usage description. A global address is acceptable.</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Regions</td>
<td>Type of Number</td>
<td>Are there ID requirements?</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>-----------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Number portability**

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>Preset UIFN times only</td>
<td>Service Provider Change Authorization and Designation of Agency provided by Amazon</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Supported Regions

<table>
<thead>
<tr>
<th>Supported Regions</th>
<th>Portability windows</th>
<th>Required Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Singapore)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe (London)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Set up outbound communications

You can send outbound communications to customers for a variety of reasons, such as appointment reminders, subscription renewals, and debt collection. Amazon Connect provides both normal and outbound campaign capabilities.

### Contents

- [Set up outbound caller ID](#)
- [Set up US emergency calling in Amazon Connect](#)
- [Enable outbound calls](#)
- [Outbound calling restrictions](#)
- [Optimize your reputation for outbound calling](#)
- [Enable Amazon Connect outbound campaigns](#)
- [Create an outbound campaign](#)
- [Disable outbound campaigns](#)
- [Security profile permissions for outbound communications](#)
Set up outbound caller ID

This topic explains how to set up your outbound caller ID name and number.

Contents

• Outbound parameters: Set in queue
• How to set the caller ID number dynamically
• Use E.164 format for international phone numbers
• How to specify a custom caller ID number using a block
• CNAM
• How to avoid labels like "spam" and "telemarketer"

Outbound parameters: Set in queue

You set the outbound caller ID name (such as the name of your company) and caller ID number in the queue settings. To edit queue settings, on the navigation menu choose Routing, Queues, and then choose the queue you want to edit.

The following image shows an Edit queue page with an arrow pointing to the Outbound caller ID name and Outbound caller ID number.
Outbound caller ID name

The **Outbound caller ID name** is set to the value that is passed from the SIP header. For example, Alice@sip:alice@example.com.

**Important**

Amazon Connect runs on a SIP-only infrastructure through our carrier partners. However, the caller ID name can be delivered to your customers only if the call path across the public telephony network is all on SIP. Because your customers are on many different networks outside of what Amazon Connect controls, the caller ID name is not guaranteed to be delivered to your customers. Depending on the country this will be up to 75% effective. To guarantee your caller ID name is delivered to customers, see [Optimize your reputation for outbound calling](#) for information about achieving it by using partner solutions.
Outbound caller ID number

Only phone numbers that you've claimed or ported to Amazon Connect can be used as your caller ID number. Outbound calls without proper identification may be blocked in certain countries such as UK and Australia.

To use an external phone number as your outbound caller ID number, contact AWS Support to see if it's possible. The phone number needs to be in a country we support for custom caller ID and you'll need to provide proof of ownership.

You can set the caller ID number as follows:

- **Call phone number block**: Use this block in an Outbound whisper flow to initiate an outbound call to a customer and, optionally, specify a custom caller ID number that is displayed to call recipients.

  This block is useful when you have multiple telephone numbers used to make outbound calls, but want to consistently display the same company phone number for the caller ID for calls made from your contact center.

  You can also use this block with the Set contact attributes block to set the callback number dynamically. For example, you can display a certain caller ID number based on the customer's account type.

- **Queue**: If no caller ID number is specified in the Call phone number block, then the caller ID in the queue settings is used.

⚠️ **Important**

Telecoms regulation limit the telephone numbers that can be used to make outbound calls in various countries. If you have set up a new number and you are not able to make outbound calls, it may be because you have configured a number that is not permitted to make outbound calls. Check our Amazon Connect Telecoms Country Coverage Guide and Region requirements for ordering and porting phone numbers.

Telecom regulations in certain countries require the carrier to identify the caller. Therefore, any unidentifiable outbound calls will be blocked. Make sure you set the Caller ID in your configurations to avoid call failures.
Toll-free numbers for caller ID

Using toll-free numbers for outbound communications have a number of limitations. For example, using a toll-free number to dial other toll-free numbers in the United States can result in the number being filtered, blocked, or not properly routed to the destination by carriers. Toll-free numbers may be terminated at a higher than expected rate. If you know you need to call toll-free numbers in the United States you must use DIDs to make the calls to be guaranteed call delivery.

If you're using toll-free numbers outside of the US, refer to the Amazon Connect Telecoms Country Coverage Guide to see which countries support toll-free numbers as outbound. For example, for Australia the guide shows it's not permitted to use toll-free numbers due to local regulations; the National Outbound column indicates that toll-free numbers are not supported.

⚠️ Important

Toll-free products are designed to be national products and phoned within the country. We do not guarantee international reachability of any of these services as access to the numbers is controlled by the caller's network access.

How to set the caller ID number dynamically

Use an attribute in the Call phone number block to set the caller ID number dynamically during the flow.

The attribute can be one you define in the Set contact attributes block in the flow. Or, it can be an external attribute returned from an AWS Lambda function.

The value of the attribute must be a phone number from your instance in E.164 format.

- If the number is not in E.164 format, the number from the queue associated with the Outbound whisper flow is used for the caller ID number.
- If no number is set for the outbound caller ID number for the queue, the call attempt will fail.

For more information about setting the caller ID dynamically, see this AWS Support Knowledge Center article: How can I set my Amazon Connect outbound caller ID dynamically based on country?
Use E.164 format for international phone numbers

Amazon Connect requires phone numbers in **E.164** format.

To express a US phone number in E.164 format, add the '+' prefix and the country code in front of the number. For example, for a US number:

- +1-800-555-1212

In the UK and many other countries internationally, local dialing requires the addition of a 0 in front of the subscriber number. However, to use E.164 formatting, this 0 must be removed. A number such as 020 718 xxxx in the UK would be formatted as +44 20 718 xxxx. When you place calls from the CCP using Amazon Connect the CCP provides the correct formatting for numbers automatically.

⚠️ Important

Phone numbers that are not formatted in E.164 will not work. They will also result in a breach of **Amazon Connect Service Terms and conditions** for acceptable use which may result in your service being suspended.

How to specify a custom caller ID number using a **Call phone number** block

1. On the left navigation menu, choose **Routing, Flows**.
2. Choose the down arrow next to **Create flow**, and then choose **Create outbound whisper flow**.
3. Add a **Call phone number** block to the flow, and connect the **Entry point** block to it.
   
   The **Call phone number** block must be placed before a **Play prompt** block if one is included in your flow.
4. Select the **Call phone number** block, and then select **Caller ID number to display**.
5. Do one of the following:
   - To use a number from your instance, choose **Select a number from your instance**, and then search for or select the number to use from the drop-down.
   - Choose **Use attribute** to use a contact attribute to provide the value for the caller ID number. You can use either a **User Defined** attribute you create using a **Set contact attributes** block, or an **External** attribute returned from an AWS Lambda function. The
value of any attribute you use must be a phone number claimed for your instance and be in E.164 format. If the number used from an attribute is not in E.164 format, the number set for the Outbound caller ID number for the queue is used.

**Important**

- The value of any attribute you use must be a phone number claimed for your instance. The number must be in E.164 format. If the number used from an attribute is not in E.164 format, calls may be terminated by the destination networks.

- It is your responsibility to ensure the numbers you are using are legally permissible. Certain numbers, such as +44870 numbers in the UK, are not legally permissible. You must ensure you're not using them.

6. Add any additional blocks to complete your flow, and connect the Success branch of the Call phone number block to the next block in the flow.

   There is no error branch for the block. If a call is not successfully initiated, the flow ends and the agent is placed in an AfterContactWork (ACW) state.

**CNAM**

As part of changes within the US Public Telephone network and a move to alternative reputation mechanisms described in Optimize your reputation for outbound calling, as of March 31, 2023, Amazon Connect no longer sets CNAM configurations.

We conducted research between January and March 2023, that showed CNAM was seen by fewer than 7% of users. This is due to changes within support for mobile providers and due to the migration to app-based reputation mechanisms.

All existing CNAM configurations set up before March 2023, are still in place. We will continue to focus on supporting modern replacement mechanisms added to our marketplace, for example, First Orion and Neustar.

**How to avoid labels like "spam" and "telemarketer"**

See the recommended steps in Optimize your reputation for outbound calling.
Set up US emergency calling in Amazon Connect

By default 911 is enabled for all users in the following North America Regions: US East (N. Virginia), US West (Oregon), and AWS GovCloud (US-West). If an agent calls 911, the call is routed through to emergency services.

What is Enhanced 911 (E911)? E911 enables location information to be sent to 911 dispatch when a 911 call is placed.

There are two steps to set up E911:

- Get and store an agent's validated physical address
- Retrieve an agent's address when they call 911

Place 911 calls from your Test Environment

⚠ Important

Calling 911 for a non-emergency situation carries a penalty of $100 per occurrence. To help you avoid penalties, we have set up 933 so you can test this capability. Calls placed from an Amazon Connect Contact Control Panel (CCP) to 933 have an audio playback message confirming:

- The number the call originated from.
- The physical address that was sent along with the call.

For more information about calling 911, see this FAQ about the national 911 program.

Get and store an agent's validated physical address

The first step in setting up E911 for your Amazon Connect instance is to get and store the agent's validated physical address. The following illustration shows the process for storing addresses.
1. Since agents may be working from different locations (for example, office building, home, or coffee shop), it's critical that the most recently validated address is passed along with the emergency outbound call.
   a. Store a validated address when you first set up an agent on Amazon Connect, based on the agent's usual location.
   b. Prompt the agent to update their address at the start of their shift to help ensure that the emergency outbound call has their latest address.
   c. Check addresses against a database of valid street addresses (Master Street Address Guide).
2. Use the Amazon Chime API `ValidateE911Address`. This API validates and returns the validated physical address.
3. Use the `CreateProfile` or `UpdateProfile` APIs to store the validated address in Amazon Connect Customer Profiles.

**Note**

We recommend using `CreateProfile` when it is required to add a validated address the first time. After that, use `UpdateProfile`.

**Retrieve an agent's address when they call 911**

To retrieve an agent's validated address from the Amazon Connect, create an outbound whisper flow that calls a Lambda function. Code the Lambda function to retrieve the address from the agent's customer profile, as shown in the following illustration:
1. Create an AWS Lambda function that uses the SearchProfiles API to retrieve the physical address for a given agent from Customer Profiles.

2. Create an outbound whisper flow that relays this physical address as part of the emergency out dial.

3. Add a task that sends notifications when an E911 call is placed.

Create an outbound whisper flow that relays the physical address

For outbound voice calls within Amazon Connect, an outbound whisper flow usually specifies the whisper to be played to customer. However, in this case you need to configure an outbound whisper flow to do the following:

1. Inspect the outbound call string from an agent.

2. If the string equals 911 (or 933 in a test environment), then retrieve the agent's stored location/physical address from Customer Profiles by using a Lambda function to call the SearchProfiles API.

3. Attach the physical address to a contact attribute and proceed with the 911 (or 933) outbound call.

The following illustration shows an example outbound whisper flow. It is configured to inspect the outbound call string from an agent, and retrieve the stored physical address for that agent by using a Lambda function. It includes the following blocks in sequence: Invoke AWS Lambda function, Set contact attributes, and Call phone number.
• Step 1: Call a Lambda function that retrieves the location for an agent (Input parameter = Agent User Name). The following image shows how to configure an Invoke AWS Lambda function block so the agent username is passed to the Lambda function.

![Invoke AWS Lambda Function](image)

• Step 2: Attach the location received to a contact attribute (see Format a physical address for E911 for the required format).

• Step 3: Update the call origination to the agent's phone number and continue with the outbound call.
Note

The origination number is the caller ID that is passed along with the 911 outbound call. If the origination phone number supports inbound calls, emergency responders will be able to call back the agent in case the initial phone call was disconnected.

- The 911 call is specific to United States. As a result, the origination phone number must be a valid US phone number.

For example, when an agent places an outbound call, if an invalid US phone number is passed to the carrier network, the carrier can reject the call. To avoid this situation, if the agent uses an invalid number from Amazon Connect, Amazon Connect defaults to the Caller ID that is assigned to the queue in the agent's routing profile.

- The capability does not place any other rules on this number. For example, the origination number can be the phone number of the security front desk.

Add a task that sends notifications when an E911 call is placed

When an agent calls 911 it is important to notify in real time the appropriate people in your organization, such as corporate security or a human resources administrator, that someone from the contact center has placed an E911 call. To do this, create an Amazon Connect task in the outbound whisper flow. Then add custom notification logic to the task.

The following image shows an example of a Create task block in an outbound whisper flow. It is located after the Set contact attributes block and before the Call phone number block.

The following image shows the Properties page for a Create task block. It is configured to notify corporate security that an agent from the contact center has placed an E911 call.
Format a physical address for E911

This topic explains how to format a physical address so it can be passed to Amazon Connect.

E911 outbound calls require a physical address to be passed to Amazon Connect as a JSON string with keys and values that represent the various fields in the address. For example, consider the following US address:

- 2121 7th Ave, Seattle, WA, 98121, USA

The address must be attached as a JSON string against the key CivicAddress, as shown in the following example. Every address field is attached to a specific coded key.

CivicAddress:
{"country":"USA","RD":"7th","A3":"Seattle","PC":"98121","HNO":"2121","STS":"Ave"

The following illustration shows how an example input address maps to PSAP address keys:
The following table shows a complete list of keys.

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Example</th>
<th>Required</th>
<th>Character limit</th>
<th>Recommended character limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>country</td>
<td>The country is identified by the two-letter ISO 3166 code.</td>
<td>US</td>
<td>Required</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>National subdivisions (state, region, province, prefecture)</td>
<td>NY</td>
<td>Required</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>City, township, shi (JP)</td>
<td>New York</td>
<td>Required</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>PRD</td>
<td>Leading street direction</td>
<td>N, W</td>
<td>Required</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>POD</td>
<td>Trailing street suffix</td>
<td>SW</td>
<td>Required</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Attribute name</td>
<td>Description</td>
<td>Example</td>
<td>Required</td>
<td>Character limit</td>
<td>Recommended character limit</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>---------</td>
<td>---------------------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>STS</td>
<td>Street suffix</td>
<td>Avenue, Platz</td>
<td>Required only if applicable to address</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>HNO</td>
<td>House number (numeric part only)</td>
<td>2121</td>
<td>Required</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>HNS</td>
<td>House number suffix</td>
<td>A, 1/2</td>
<td>Required only if applicable to address</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>LOC</td>
<td>Additional location information</td>
<td>Room 543</td>
<td>Optional</td>
<td>60</td>
<td>20 or less</td>
</tr>
<tr>
<td>NAM</td>
<td>Name (residence, business or office occupant)</td>
<td>Example Corp</td>
<td>Optional</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>PC</td>
<td>Postal code</td>
<td>10027</td>
<td>Required</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>RD</td>
<td>Primary road or street</td>
<td>Broadway</td>
<td>Required</td>
<td>40</td>
<td></td>
</tr>
</tbody>
</table>
Note
It is your responsibility to validate the address against a standard repository such as the Master Street Address Guide (MSAG).

Programming notes

Currently it isn't possible to pass a JSON structure as an Attribute to Amazon Connect. Therefore, the location retrieved by the Lambda function needs to be converted to a JSON string before it is passed to Amazon Connect. For example, using the Python programming language, if the location retrieved is stored in a JSON structure `json_agent_location` then it can be passed to Amazon Connect (from the Lambda function) as follows:

```python
return { 'CivicAddress': json.dumps(json_agent_location), 'agent_did_number': '+15555551212' }
```

For an address such as the following example:

- 2121 7th Ave, Seattle, WA, 98121, USA

The key-value pair:

```json
CivicAddress: {"country": "USA", "RD": "7th", "A3": "Seattle", "PC": "98121", "HNO": "2121", "STS": "Ave", "A1": "WA"}
```

And the corresponding JSON string that is actually passed to Amazon Connect:

```json
CivicAddress: {"country": "USA", "RD": "7th", "A3": "Seattle", "PC": "98121", "HNO": "2121", "STS": "Ave", "A1": "WA"}
```

Note
Using `json.dumps` adds an escape character \ to each quotation mark (").

Enable outbound calls

Before your agents can make outbound calls to customers, you need to set up your Amazon Connect instance for outbound communications.
1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose Telephony.

4. To enable outbound calling from your contact center, choose Make outbound calls with Amazon Connect.

5. To enable outbound campaigns, choose Enable outbound campaigns.

6. By enabling early media audio, your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages from telephony providers, when making outbound calls. Choose Enable early media.

7. Choose Save.

8. Ensure agents have the Contact Control Panel (CCP) - Make outbound calls permission in their security profile. For instructions, see Assign a security profile to a user.

---

Note

For a list of countries you can call by default based on the Region of your instance, see Countries you can call by default.

For a list of all countries available for outbound calls based on the Region of your instance, see Amazon Connect pricing. If a country is not available in your dropdown menu, open a ticket to add it to your allowlist.
Outbound calling restrictions

This topic explains restrictions that are in place for outbound calling with Amazon Connect.

Contents

- Use of toll-free numbers outside the country of origin
- Use of UIFN numbers for outbound dialing
- Redirection of calls
- International calling restrictions

Use of toll-free numbers outside the country of origin

Amazon Connect does not support the use of toll-free numbers for international calling. International calls from toll-free numbers can be flagged as spam by downstream providers, resulting in negative reputation scores. They can also generate unexpected fees for call recipients.

Use of UIFN numbers for outbound dialing

UIFN numbers are designed to be used for inbound calls only. They cannot be used for outbound calling. If you attempt to use UIFN for outbound calling, the calls will be blocked.

Redirection of calls

If you are using Amazon Connect to redirect calls: If you are receiving calls with Anonymous (withheld CLI), you must use an Amazon Connect number for the transfer. See Set up outbound caller ID.

International calling restrictions

Amazon Connect has several restrictions on international calling. These are based on requirements in the following specific jurisdictions.

South Africa

South African mobile numbers available under the DID option are designed to be national-only services and are not supported for international calling.

Taiwan

Taiwan DID's are set up to be in-country only services and are not internationally reachable.
China

Chinese carriers are increasingly blocking international routes into China unilaterally. Amazon Connect has taken steps to continue to support our existing customers but require that all customers comply with additional requirements for continued use. Starting October 14, 2023 all customers approved to call China are required to follow these conditions.

Eligibility criteria

- **Unsupported use cases**
  - Short calls and alerting (less than 15 seconds).
  - High volume of calls, especially when done over a short period of time, using the same outbound caller ID (more than 5 calls per minute).
  - Any form of cold calling.
  - Any calls to invalid phone numbers. All numbers called must be validated as accurate.
  - Repeated calls using the same FROM / TO numbers.
  - Attempts to call China FROM any number that has not been pre-approved.

- **Supported use cases**
  - Direct calls to known business entities. For example, calling a hotel or IT support function.
  - Calling users who attempted to engage with your business. For example, university placement schemes or product purchases.

Data required for setup

To request the ability to call Chinese telephone numbers (+86), perform the following steps:

- You must provide a exact list of telephony numbers you will use to phone China.
  - The number must be a DID provided by Amazon Connect. No other number is acceptable.
  - The number cannot be a DID provided by Hong Kong, Macau, Taiwan, China, or Singapore.

Note

The above list may change at any time.
• Any number used to call Chinese telephone numbers must be able to called back. You must also implement a call back message that clearly states the name of the company that is associated with the phone number.

• You must provide a detailed description of your use case, and confirm that you meet the eligibility criteria described in this topic.

Consequences for violating the calling criteria for China

Amazon Connect has a zero tolerance policy for calling into China. Amazon will suspend your use of Amazon Connect if you use the service for any of the restricted use cases identified in this topic. It is essential that the administrators of your Amazon Connect service focus on ensuring the members of your organization are aware of these restrictions, as ignorance of the rules is not an acceptable reason for breach.

Service assurance

In the event of further incidents where Chinese carriers block major international routes without prior warning and impact the ability to call China, the exemptions in the Amazon Connect Service Level Agreement will take effect.

Optimize your reputation for outbound calling

In the contact center industry one of the most difficult tasks is understanding why customers don't answer calls when you dial out. Is the customer deliberately not answering, or are they busy on a work call or answering the door? For contact centers it's impossible to know but there are things you can do about it.

This topic provides recommended steps you can take to improve your call answer rates for outbound calling.

Step 1: Know your customer's preferred contact method

One of the biggest mistakes that contact centers make is not knowing whether the customer wants to be contacted by telephone call. When the customer engaged with you, did you check whether they want to be reached by phone, e-mail, or text?

Businesses with multi-channel engagement outperform 70% on average compared to business without multi-channel engagement.
Step 2: Brand your calls

By using call branding solutions, you can provide enhanced call displays that include your business name, logos, reason for the call, and your service. Branding your calls increases the call answer it by 30%.

Amazon Connect partners with solutions providers like First Orion and Neustar to offer branded calling services. To discuss the services directly with our partners, visit their dedicated Amazon Connect website:

- First Orion.
- Neustar.

Step 3: Select caller IDs that mean something to your customer

Not every contact center is the same. What works for some might not work for others. But there are correlations in how successful outbound campaigns are based on your caller ID. Following are a few suggestions to try creating meaningful caller IDs:

- Area localization. Use a caller ID in the same area as the prospect.
- City localization. Use a caller ID in the same city as the prospect.
- Recognizable golden toll free number such as 0800 123 0000.
- Mobile numbers. Where countries permit this, it may be possible to use a virtual mobile number to dial out from a contact center. For a list of countries where Amazon Connect supports mobile numbers, see Region requirements for ordering and porting phone numbers.

Step 4: Make sure your campaign is calling valid numbers

Many businesses don't have a process to ensure that customer details are up to date. With people being more mobile than ever, it's essential for businesses to keep updated contact information. If customers are not answering your calls, we recommend using Amazon Pinpoint to validate your phone numbers. It may be the customer is no longer at the phone number you are calling.

Step 5: Make outbound calls at optimal times

Another strategy for outbound call campaigns is making sure that calls are placed at the best times. It is critical to never harass your customers or prospects—no one wants to be contacted multiple times by the same company. Generally speaking, it is never a good idea to call before
10:00AM or after 5:00PM as people are at their busiest or need their quiet time. Customers should be called when it's a good for them, depending on their profile. This may mean that one customer should be called around noon, while another is more accessible in the afternoon.

In addition, there are regulations such as TCPA (in the US) and OFCOM (in the UK) that provide guidance on when not to call end customers. We strongly recommend that you abide by such regulations.

**Step 6: Monitor the reputation of your caller IDs**

We recommend monitoring the reputation of your caller ID through a service like Free Caller Registry.

Even with the most legitimate outbound call campaigns, if you make enough calls, there will be people who will flag your caller ID as spam. This can manifest in two ways:

1. **Automatic blocking.** Block lists are implemented on a vendor-by-vendor basis. For example, when a certain threshold of reports is reached with application providers such as Hiya.com on Samsung devices, up to 20% of your prospects will become instantly unreachable.

2. **Complaints.** There are numerous websites where people complain about calls from specific caller IDs. A number of your prospects will search your caller ID online when you call them. If it has a bad reputation, they will be less likely to answer.

The fastest way to recover from a flagged caller ID is to switch to a new phone number. See the next step.

**Step 7: Use multiple numbers as a callerID**

Today, outbound contact centers typically embrace an intelligent, more efficient manner of dialing.

For example, one method is to use multiple phone numbers when placing outbound calls. Customers are more likely to answer a call if they feel that they are not being called repeatedly by the same number. In fact, using the same phone number repeatedly is a sure way to annoy customers and prospects who may feel they are being contacted too often.

**Step 8: Engage with App Vendors**

One of the most difficult issues with the industry as it currently stands is that a large number of vendors provide in-app services to block calls. If one of these in-app services marks your number as spam then you have to pay the premium fees to remove your number from their spam list.
Some of the third party vendors are joining in partnership to increase the call answer rate.

**Step 9: Add messaging to your outreach strategy to let customers know who you are**

It's inevitable that you'll end up with a list of unanswered calls that you weren't able to connect. There are a variety of creative ways to use SMS with prospects. Here are some ideas to increase answer rates with your prospects.

1. Send an SMS before calling, letting them know who you are and when you will be calling, optionally allowing them to reschedule to a more convenient time.
2. If the prospect doesn't answer, send an SMS to allow them to reschedule the call or request a call back.
3. Re-engage with prospects with promotional offers or discounts that resonates with your prospects.

**Step 10: Validate your outbound calling strategy**

By making data-driven decisions and continuously iterating, you'll have the best chance to deliver real business value. You should treat each change that you make to your outbound calling strategy as an experiment, and ensure you have the ability to measure and compare the effectiveness of the changes you are making.

One of the best things with Amazon Connect is the service is readily available to experiment. You can establish a baseline and then compare any changes to help you to assess how you can succeed.

**Enable Amazon Connect outbound campaigns**

This topic explains how to enable Amazon Connect outbound campaigns, a feature of Amazon Connect and formerly known as high-volume outbound communications.

**Important**

The phone numbers that outbound campaigns can call are based on the AWS Region where your Amazon Connect instance is created. For a list of AWS Regions and countries, see [Outbound campaigns](#) in the *Availability of Amazon Connect services by Region* topic.
Before you begin

There are a few things that you need in place before using outbound campaigns:

- Make sure your instance is enabled for outbound calling.
- Create a dedicated outbound campaigns queue to handle any contacts that will be routed to agents as a result of the campaign.
- Assign the queue to the agent's routing profile.
- Create and publish a flow that includes a Check call progress block. This block enables you to branch based on whether a person answered the phone, for example, or a voicemail was detected.

ℹ️ Note

If you plan to call customers in Australia or New Zealand, see Step 4: Create a new campaign in the Amazon Connect instance in this blog for instructions: Make predictive and progressive calls using Amazon Connect outbound campaigns.

Create a AWS KMS key

When you enable outbound campaigns, you have the option to provide your own AWS KMS key. These keys are created and managed by you (AWS KMS charges apply). You also have the option to use an AWS owned key.

When enabling or disabling outbound campaigns using an API, make sure the API user is either the administrator or has the following permissions: kms:DescribeKey, kms:CreateGrant, and kms:RetireGrant for the key.

ℹ️ Note

To switch the KMS key that is associated with outbound campaigns, first you need to disable outbound campaigns, and then re-enable it using a different AWS KMS key.

Configure outbound campaigns

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose Telephony.

4. To enable outbound campaigns, choose Enable outbound campaigns. If you don’t see this option, then check whether outbound campaigns is available in your AWS Region.

5. Under Encryption settings, enter your own AWS KMS key or choose Create an AWS KMS key.

If you choose Create an AWS KMS key:

- A new tab in your browser opens for the Key Management Service (KMS) console. On the Configure key page, choose Symmetric, and then choose Next, as shown in the following image.

  ![Configure key image]

  - On the Add labels page, add a name and description for the key, and then choose Next.
  - On the Define key administrative permissions page, choose Next.
• On the Define key usage permissions page, choose Next.

• On the Review and edit key policy page, choose Finish.

In the following example, the name of the key starts with **bcb6fdd**:

![KMS Customer managed keys](image)

• Return to the tab in your browser for the Amazon Connect console, Telephony page. Click or tap in the AWS KMS key for the key you created to appear in a dropdown list. Choose the key you created.

6. Choose **Save**.

7. It takes a few minutes for outbound campaigns to be enabled. When it's successfully enabled, you can create outbound campaigns in Amazon Connect for voice calls. If it does not enable, verify you have the required **IAM permissions**.

**Create an outbound campaign**

Contact centers send outbound campaigns to customers for a variety of reasons, such as appointment reminders, telemarketing, subscription renewals, and debt collection. By using Amazon Pinpoint Journeys and Amazon Connect, you can create outbound campaigns for voice, SMS, and email.

There are two ways you can create an outbound campaign:

• Use Amazon Connect console and Amazon Pinpoint. This topic provides instructions.

• Use the Amazon Connect Outbound Campaigns API. For more information, see [Amazon Connect Outbound Campaigns API Reference](#).

**Note**

• You can't update the name of the outbound queue by using the API.
When you create a campaign by using the API: For users to be able to view or edit a campaign at a later date by using the Amazon Connect user interface, you must add the instance ID as a tag.

How to create an outbound campaign

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. On the left navigation menu, choose Outbound campaigns, and then choose Create campaign.
3. In the Campaign details section, specify the name, as shown in the following image.

4. In the Outbound configuration section, select the published flow you created for outbound campaigns (a flow that includes a Check call progress block), as shown in the following image.
5. If you plan on using Predictive or Progressive dialer types, specify a queue to associate with this campaign. A queue is required only for Predictive and Progressive dialer types.

6. Answering machine detection is enabled by default. If desired, you can choose to disable it.

⚠️ **Note**

To reduce call connection latency between your customers and available agents we recommend disabling the use of answering machine detection. For additional best practices, see this blog: [Amazon Connect – Best practices for running outbound campaigns](https://example.com).

If you disable answering machine detection, and if your flow includes the [Check call progress](https://example.com) block, the contact is routed down the Error branch.

7. Choose a phone number to be shown as caller ID when making outbound calls. The outbound phone number is specified for a queue.

⚠️ **Important**

- You must use a phone number that has been ported to your Amazon Connect instance, or claimed from Amazon Connect.
- Telecom regulations in certain countries dictate use of phone numbers from specific carriers for outbound calling. For more information, see the [Amazon Connect Telecoms Country Coverage Guide](https://example.com) to learn more.
- If you plan to call customers in Australia or New Zealand, see **Step 4: Create a new campaign in the Amazon Connect instance** in this blog for instructions: [Make predictive and progressive calls using Amazon Connect outbound campaigns](https://example.com).

8. In the **Dialer type** section, choose a dialer type.
9. If you’re using a Predictive or Progressive dialer type, choose the Agent bandwidth allocation. This setting applies to Predictive and Progressive dialer types only. It doesn’t apply to Agentless mode.

10. Choose Dialing capacity.

11. Open the Amazon Pinpoint console (https://console.aws.amazon.com/pinpoint/) and Create a journey, using the name of the campaign that you created in Amazon Connect.

12. Associate this campaign to a customer journey on Amazon Pinpoint to start making high-volume outbound calls.

**Campaign state**

After a campaign is running, you can pause or stop it. You can also delete a campaign at any time.

Following is a description of each campaign state:

- **Created** – The campaign is created.
- **Running** – The campaign as running.
- **Paused** – The campaign is paused until it is resumed.
- **Stopped** – The campaign is stopped. You can't resume a campaign that is stopped.
- **Failed** – An error state caused the campaign to fail.
Disable outbound campaigns

⚠️ Important
You must delete all existing campaigns before you can disable outbound campaigns.

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose Telephony.
4. To disable outbound campaigns, uncheck Enable outbound campaigns.
5. Choose Save.

   You can no longer create outbound campaigns.

Security profile permissions for outbound communications

To enable agents to make outbound calls, assign Make outbound calls permissions to the agent's security profile as shown in the following image:
To enable call center managers to create outbound campaigns, assign the **outbound campaigns** permissions to their security profile.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

By default, the **Admin** security profile already has permissions to perform all activities.

**Manage users in Amazon Connect**

As the admin one of your key responsibilities is to manage users, add users to Amazon Connect, give them their credentials, and assign the appropriate permissions so they can access the features needed to do their job.

The topics in this section explain how to add users using the Amazon Connect admin website. To manage users programmatically, see [User management actions](#) in the *Amazon Connect API Reference Guide*.

**Contents**

- [Add users to Amazon Connect](#)
- [Edit users in bulk](#)
- [View historical changes to user records](#)
- [Download users from your Amazon Connect instance](#)
- [Delete users from your Amazon Connect instance](#)
- [Reset a user’s password for Amazon Connect](#)
- [Security profiles](#)
Add users to Amazon Connect

When you add users to Amazon Connect, you can configure them with information appropriate to their roles. For example, you specify their security profile, which indicates the tasks they can perform in Amazon Connect admin website. For agents you specify their routing profile, which indicates the contacts that can be routed to them.

This topic explains how to add users using the Amazon Connect admin website. To add users programmatically, see CreateUser in the Amazon Connect API Reference Guide. To use the CLI, see create-user.

Add a user individually

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Users - Create permission.
2. In Amazon Connect, on the left navigation menu, choose Users, User management.
3. Choose Add new users.
4. Choose Create and set up a new user and then choose Next.
5. Enter the name, email address, secondary email address, mobile number, and password for the user.

Note

The following caveat only applies to Amazon Connect instances that are not configured for SAML, that is, instances where you chose Store users in Amazon Connect when you configured identity management for your instance:

- If you provide a secondary email, the user receives email notifications - other than password reset notifications - to this email address instead of to their primary email address.

Tip

Mobile number is not currently used by Amazon Connect.

6. Choose a routing profile and a security profile.
7. Optionally, add resource tags to identify, organize, search for, filter, and control who can access this user.

8. Choose **Save**. If the Save button isn't active, it means you're logged in with an Amazon Connect account that doesn't have the required security profile permissions.

   To fix this issue, log in with an account that is assigned to the Amazon Connect Admin security profile. Or, ask another Admin to help.

9. For information about adding agents, see [Configure agent settings: routing profile, phone type, and auto-accept calls](#).

### Add users in bulk from a .csv file

**Note**

Avoid adding too many unique resources in the .csv file. For example, don't add more than 100 different routing profiles. This may cause a timeout or failure during the validation process.

Bulk upload is for adding new records, not for editing existing records. To edit user records in bulk, see [Edit users in bulk](#).

Use these steps to add several users from a .csv file such as an Excel spreadsheet.

1. Log in to Amazon Connect with an **Admin** account, or an account assigned to a security profile that has **Users - Create** permission.

2. In Amazon Connect, on the left navigation menu, choose **Users, User management**.

3. Choose **Add new users**.

4. Choose **Import users using a .csv template** and then choose **.csv template**.

   The .csv template has the following columns in the first row:

   - first name
   - last name
   - email address
   - secondary email address
   - mobile: This is not currently used by Amazon Connect.
- password
- user login
- agent hierarchy
- routing profile name
- security_profile_name_1|security_profile_name_2
- user_hierarchy_1|user_hierarchy_2
- phone type (soft/desk)
- phone number
- soft phone auto accept (yes/no)
- ACW timeout (seconds)
- tags

The following image shows a sample of what the .csv template looks like in an Excel spreadsheet. The first row in the spreadsheet contains the column headings, and the second row contains sample user data.

5. Add your users to the template and upload it to Amazon Connect. Choose **Upload file and verify**.

6. Amazon Connect validates the data in the file. Choose **Save** to create the new user records.
If you get a validation error message, it usually indicates that one of the required columns is missing information, or there's a typo in one of the cells.

The following image shows an example validation error message. In this case, the security profile was misspelled and a password didn't meet requirements.

7. To upload only the validated user records, choose **Save**. A dialog box prompts you for confirmation.
8. A banner displays the status of the upload and confirms when it's complete.

**Tip**

While a batch of additions is being processed, you can continue working on the **User management** page, choosing another batch of user records to create, edit, or delete, in bulk or individually. This is useful for quickly updating settings such as routing profiles for groups of agents. Amazon Connect sequentially processes the records in bulk.

9. Choose **Refresh** to update the **User management** page with the users that have been created.

**Required permissions for adding users**

Before you can add users to Amazon Connect, you need the following permissions assigned to your security profile: **Users - Create**. The following image shows that this security profile permission is in the **Users and permissions** section of the **Add/Edit security profile** page.
By default, the Amazon Connect Admin security profile has these permissions.

For information about how to add more permissions to an existing security profile, see Update security profiles.

**Edit users in bulk**

Bulk edit mode enables you to quickly edit the attributes that are common across user records, such as routing profiles, security profiles, and tags.

---

<table>
<thead>
<tr>
<th>Users</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Remove</th>
<th>Enable/Disable</th>
<th>Edit permission</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent hierarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1. Log in to Amazon Connect with an Admin account, or an account assigned to a security profile that has Users - Edit permission.
2. In Amazon Connect, on the left navigation menu, choose Users, User management.
3. If needed, choose Add filter to specify a subset of users, such as users with a specific Routing profile. This option is shown in the following image.

---

**Tip**

While a batch of bulk edits is being processed, you can continue working on the User management page, such as selecting more records to edit or delete, in bulk or individually. This is useful for quickly updating settings, such as routing profiles for groups of agents.
4. To quickly update a large number of users, at the bottom of the table choose to display **100** rows per page, as shown in the following image.

5. To edit all the records on the page, choose the top box. Otherwise, select one or more records you want to edit at the same time. Choose **Edit**.

6. On the **Bulk edit** page, in the **Settings** section, you can choose the following settings for all of the selected users:
• Security profile
• Routing profile
• Phone type
• After Call Work (ACW) timeout
• Agent hierarchy, if this has been set up
• Tags

7. Choose Save to apply your changes to the selected records.

8. While that batch of user records is being updated, you can continue working on the User management page, performing other create, edit, and delete tasks on user records.

Perform other edit tasks while a batch of bulk edits is being processed

After saving an update for a group of users, you can either make additional changes on the Bulk edit page (for example, edit other user details such as contact information) or you can choose different user records to edit.

⚠️ Important

As long as you remain on the User management page, your update request will continue to be processed. Review the messages at the top of the page for the status of the update.

The following image shows an example of message at the top of the User management page that Amazon Connect is updating a batch of user records.

When you perform additional tasks on the User management page, Amazon Connect appends the next request to create, edit, or delete user records to the existing status message at the top of the page. Amazon Connect sequentially processes them in bulk.

Following are some tips about how Amazon Connect processes bulk edit requests.
• If you choose **Cancel** during a bulk create, edit, or delete, **only those requests not yet processed are canceled**.

• A message displays how many users were successfully updated. Choose **Refresh** to refresh the page with the list of the updated users.

![Refresh](image)

• If some user records fail to be updated, a message similar to the following image is displayed:

![Failed to update 3 users](image)

You have the following options:

• Choose **download the CSV** to discover the reason changes weren't updated. In the following example, the agent hierarchy was deleted before the user records were saved.

![CSV download](image)

• Choose **Try again** to resubmit only those user records that failed. The others were already successfully updated.

• Choose **Edit** to be directed to the **Bulk edit** page so you can change the input for the user records that failed.

![Bulk edit](image)

• Choose **Cancel** to not do anything with the 3 user records that weren't updated.
Edit other user details

You can page through selected user records to make updates to contact information, rather than choosing and opening each record individually.

1. On the **Bulk edit** page, select the user records you want to edit.
2. Choose the **Edit** (pencil) icon next to individual users to make updates.
3. A dialog box opens for the individual user. Make your changes, and choose **Submit**.
4. If needed, choose **Previous** and **Next** to open the next user record in the list. The following image shows the **Edit** dialog box for a single user while in bulk edit mode.

![Edit dialog box for a single user while in bulk edit mode](image)

Edit user settings programmatically

You can change the following values programmatically across selected users. The users are changed to the same value.

<table>
<thead>
<tr>
<th>Property</th>
<th>API</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing profiles</td>
<td><a href="#">UpdateUserRoutingProfile</a></td>
<td><a href="#">update-user-routing-profiles</a></td>
</tr>
<tr>
<td>Tags</td>
<td><a href="#">TagResource</a></td>
<td><a href="#">tag-resource</a></td>
</tr>
</tbody>
</table>
You can edit the following identity and contact information programmatically for an individual user: first name, last name, username, email address, secondary email address, country code, and alternative email address for notifications. Use the following API or CLI:

<table>
<thead>
<tr>
<th>Property</th>
<th>API</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and contact information</td>
<td>UpdateUserIdentityInfo</td>
<td>update-user-identity-info</td>
</tr>
</tbody>
</table>

**View historical changes to user records**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Users and permissions - Users - View permissions.
2. In Amazon Connect, on the left navigation menu, choose Users, User management.
3. On the User management page, choose View historical changes, as shown in the following image.
4. On the **View recent changes for agent** page, there is one row for each time a user record was changed. In the following image, there are multiple rows for **johndoe** because that user record has been updated multiple times.

To view the past changes for a specific user, choose their user name.

5. On the **View recent changes for [resource name]** page, you can view details about what has been changed in the user record, when, and who made the change, as shown in the following image.
Download users from your Amazon Connect instance

You can export a list of users from Amazon Connect to a .csv file. The output is limited to the results that appear on the page; it does not include all the users, if you have more users than appear on the page.

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Users and permissions - Users - Edit permissions.
2. In Amazon Connect, on the left navigation menu, choose Users, User management.
3. Choose Download CSV.

Tip

If a user has Users - View permissions instead of Edit permissions, they will see the Download CSV option on their page, but when they choose it, the .csv file will be empty.

Delete users from your Amazon Connect instance

Important

- You can’t undo a deletion.
When a user is deleted from Amazon Connect, you won't be able to configure their agent settings any more. For example, you won't be able to assign a routing profile to them.

This topic explains how to delete user records using the Amazon Connect admin website. To delete user records programmatically, see `DeleteUser` in the *Amazon Connect API Reference Guide*. To use the CLI, see `delete-user`.

**What happens to the user's metrics?**

The user's data in contact records and reports is retained. The data is preserved for the consistency of the historical metrics. For example, when you search for contact records, you'll still see the agent's username, any contact recordings involving the agent, etc.

In the historical metrics reports, the agent's data will be included in the *Agent performance* metrics report. However, you won't be able to see an *Agent activity audit* of the deleted agent because their name won't appear in the drop-down list.

**How to delete users**

1. Log in to Amazon Connect using an **Admin** account, or an account assigned to a security profile that has **Users - Remove** permission.
2. In Amazon Connect, on the left navigation menu, choose **Users, User management**. Choose one or more users you want to delete, and then choose **Delete**.
3. Confirm you want to delete the users.

4. The following image shows an example of the message when a user is deleted successfully. Choose Refresh to update the list of users on the User management page.

5. If Amazon Connect fails to delete one or more user records, it displays a message similar to the following image.
When you get a failed to delete message, you have the following options:

- Choose **download the CSV** to view the error details. The following details show the user records had already been deleted. In this case, I hadn't refreshed the **User management** page and tried to delete the records again.

```
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login</td>
</tr>
<tr>
<td>2</td>
<td>batch100</td>
</tr>
<tr>
<td>3</td>
<td>batch101</td>
</tr>
<tr>
<td>4</td>
<td>batch102</td>
</tr>
<tr>
<td></td>
<td>Failed reason</td>
</tr>
<tr>
<td></td>
<td>The specified user was not found</td>
</tr>
<tr>
<td></td>
<td>The specified user was not found</td>
</tr>
<tr>
<td></td>
<td>The specified user was not found</td>
</tr>
</tbody>
</table>
```

- Choose **Try again** to resubmit those records that failed to be deleted. The other records were successfully deleted.
- Choose **Cancel** to not do anything with the user records that weren't deleted.

**Required permissions to delete users**

Before you can update permissions in a security profile, you must be logged in with an Amazon Connect account that has the following permissions: **Users - Remove**.
By default, the Amazon Connect Admin security profile has these permissions.

**Reset a user's password for Amazon Connect**

**To reset a user's Amazon Connect password**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or a user account that has security profile permissions to reset passwords.
2. In Amazon Connect, on the left navigation menu, choose Users, User management.
3. Select the user and choose Edit.
4. Choose reset password. Specify a new password and then choose Submit.
   
   Resetting the user's password will immediately log them out of the Contact Control Panel.
5. Communicate the new password to the user.

**Reset your own lost or forgotten Amazon Connect admin password**

- See Emergency admin login.
Reset your own agent or manager password

Use the following steps if you want to change your password, or if you forgot it and need a new one.

1. If you're an Amazon Connect agent or manager, at the Amazon Connect login page, choose Forgot Password.
2. Type the characters you see in the image, and then choose Recover Password.
3. A message will be sent to your email address with a link that you can use to reset your password.

Reset your own lost or forgotten AWS password

- To reset the password you used when you first created your AWS account, see Resetting a Lost or Forgotten Root User Password in the IAM User Guide.

Security profiles

A security profile is a group of permissions that map to a common role in a contact center. For example, the Agent security profile contains permissions needed to access the Contact Control Panel (CCP).

Security profiles help you manage who can access the Amazon Connect dashboard and Contact Control Panel (CCP), and who can perform specific tasks.

Contents

- Best practices for security profiles
- About inherited permissions
- List of security profile permissions
- Default security profiles
- Assign a security profile to a user
- Create a security profile
- Update security profiles
- Tag-based access control
Best practices for security profiles

- **Limit who has Users - Edit or Create permissions**

  People with these permissions pose a risk to your contact center because they can do the following:

  - Reset passwords, including that of the administrator.
  - Grant other users permission to the Admin security profile. People assigned to the Admin security profile have full access to your contact center.

  Doing these things would enable someone to lock out those who need to access Amazon Connect, and allow in others who can steal customer data and damage your business.

  To reduce the risk, as a best practice we recommend limiting the number of people who have Users - Edit or Create permissions.

- **Use AWS CloudTrail** to log the requests and responses of UpdateUserIdentityInfo. This enables you to track changes made to user information. Someone who has the ability to call the UpdateUserIdentityInfo API can change a user's email address to one owned by an attacker, and then reset the password through email.

- **Understand inherited permissions**

  Some security profiles included inherited permissions: when you assign dedicated permissions to one object, by default permissions are granted to sub-objects. For example, when you grant dedicated permission to edit users, you also grant them permission to list all security profiles for your Amazon Connect instance. This because to edit users, the person has access to drop-down list of security profiles.

  Before assigning security profiles, review the list of inherited permissions.

- **Understand the implications of access control tags before applying them to a security profile.**

  Applying access control tags is an advanced configuration feature that is supported by Amazon Connect and that follows the AWS shared responsibility model. Ensure that you have read the documentation and understand the implications of applying granular permission configurations. For more information, please review the [AWS shared responsibilities model](#).

- **Track who accesses recordings.**
In the **Analytics and Optimization** permission group, you can enable a download icon for recorded conversations. When members of this group go to Analytics and optimization, **Contact search**, and then search contacts, they will see an icon to download recordings.

⚠️ **Important**

This setting isn't a security feature. **Users who don't have this permission can still download recordings using other less-discoverable ways.**

We recommend that you track who in your organization accesses recordings.

**About inherited permissions**

Some security profiles included inherited permissions: when you give a user explicit permissions to **View** or **Edit** one resource type, such as queues, they implicitly inherit permissions to **View** another resource type, such as phone numbers.

For example, assume you explicitly grant someone permission to **Edit/View** queues, as shown in the following image:

![Security profile permissions](image)

By doing this you also implicitly grant them permissions to **View** a list of all phone numbers and hours of operation in your Amazon Connect instance, **when they add them to the queue**. On the **Add new queue** page, the available phone numbers and hours of operation appear in dropdown lists, as shown in the following image.
However, the user doesn't have permissions to **Edit** the phone numbers and hours of operation.

In this case, they also don't inherit permissions to **View** contact flows (the outbound whisper flow) and quick connects because those resources are optional.

**List of inherited permissions**

The following table lists permissions that are implicitly inherited when you assign dedicated permissions to a user.

**Tip**

When a user has only explicit **View** permissions and not also **Edit** permissions, the objects are retrieved but Amazon Connect doesn't surface them in drop-down lists for the user to peruse.

<table>
<thead>
<tr>
<th>Dedicated permission</th>
<th>Inherited permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users - View or Edit</td>
<td>When someone edits a user's information in the Amazon Connect console, they can <strong>view</strong> the following information in drop-down boxes when they add it to the user's account:</td>
</tr>
</tbody>
</table>
### List of security profile permissions

The security profile permissions in Amazon Connect allow users access to perform specific tasks in Amazon Connect.

The following tables list:
- **UI name**: The name of the permission as it appears on the Security profiles page in Amazon Connect.

- **API name**: The name of the permission when it is returned by the ListSecurityProfilePermissions API.

- **Use**: The functionality granted by the permission.

## Routing

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick connects - Create</td>
<td>TransferDestinations.Create</td>
<td>Create quick connects.</td>
</tr>
<tr>
<td>Quick connects - Delete</td>
<td>TransferDestinations.Delete</td>
<td>Delete quick connects.</td>
</tr>
<tr>
<td>Quick connects - Edit</td>
<td>TransferDestinations.Edit</td>
<td>Edit quick connects.</td>
</tr>
<tr>
<td>Quick connects - View</td>
<td>TransferDestinations.View</td>
<td>View quick connects. Agents need this permission so they can view quick connects in the agent application to transfer calls.</td>
</tr>
<tr>
<td>Hours of operation - Create</td>
<td>HoursOfOperation.Create</td>
<td>Set hours of operation and timezone for a queue.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>HoursOfOperation - Delete</td>
<td>HoursOfOperation.Delete</td>
<td>Delete hours of operation and timezone for a queue.</td>
</tr>
<tr>
<td>HoursOfOperation - Edit</td>
<td>HoursOfOperation.Edit</td>
<td>Edit hours of operation and timezone for a queue.</td>
</tr>
<tr>
<td>HoursOfOperation - View</td>
<td>HoursOfOperation.View</td>
<td>View hours of operation and timezone for a queue.</td>
</tr>
<tr>
<td>Queues - Create</td>
<td>Queues.Create</td>
<td><a href="#">Create queues</a></td>
</tr>
<tr>
<td>Queues - Edit</td>
<td>Queues.Edit</td>
<td>Edit information for a queue, such as name, description, and hours of operation.</td>
</tr>
<tr>
<td>Queues - Enable / Disable</td>
<td>Queues.EnableAndDisable</td>
<td><a href="#">Enable and disable queues</a> to quickly control the flow of contacts to queues temporarily.</td>
</tr>
<tr>
<td>Queues - View</td>
<td>Queues.View</td>
<td>View a list of queues in your Amazon Connect instance.</td>
</tr>
<tr>
<td>Task templates - Create</td>
<td>TaskTemplates.Create</td>
<td><a href="#">Create task templates</a></td>
</tr>
<tr>
<td>Task templates - Delete</td>
<td>TaskTemplates.Delete</td>
<td>Delete task templates.</td>
</tr>
<tr>
<td>Task templates - Edit</td>
<td>TaskTemplates.Edit</td>
<td>Edit task templates.</td>
</tr>
</tbody>
</table>
## Channels and flows

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task templates - View</td>
<td>TaskTemplates.View</td>
<td>View task templates.</td>
</tr>
<tr>
<td>Prompts - Create</td>
<td>Prompts.Create</td>
<td>Create prompts.</td>
</tr>
<tr>
<td>Prompts - Delete</td>
<td>Prompts.Delete</td>
<td>Delete prompts.</td>
</tr>
<tr>
<td>Prompts - View</td>
<td>Prompts.View</td>
<td>View a list of available prompts.</td>
</tr>
<tr>
<td>ContactFlows - Create</td>
<td>ContactFlows.Create</td>
<td>Create flows.</td>
</tr>
<tr>
<td>ContactFlows - Delete</td>
<td>ContactFlows.Delete</td>
<td>Delete flows.</td>
</tr>
<tr>
<td>ContactFlows - Edit</td>
<td>ContactFlows.Edit</td>
<td>Edit flows.</td>
</tr>
<tr>
<td>ContactFlows - Publish</td>
<td>ContactFlows.Publish</td>
<td>Publish flows.</td>
</tr>
<tr>
<td>ContactFlows - View</td>
<td>ContactFlows.View</td>
<td>View flows.</td>
</tr>
<tr>
<td>Flow modules - Create</td>
<td>ContactFlowModules.Create</td>
<td>Create flow modules for reusable functions.</td>
</tr>
<tr>
<td>Flow modules - Delete</td>
<td>ContactFlowModules.Delete</td>
<td>Delete flow modules.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Flow modules - Publish</td>
<td>ContactFlowModules.Publish</td>
<td>Publish flow modules.</td>
</tr>
<tr>
<td>Phone numbers - Claim</td>
<td>PhoneNumbers.Claim</td>
<td>Claim phone numbers.</td>
</tr>
<tr>
<td>Phone numbers - Edit</td>
<td>PhoneNumbers.Edit</td>
<td>Edit phone numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attach a claimed or ported phone number to a flow.</td>
</tr>
<tr>
<td>Phone numbers - Release</td>
<td>PhoneNumbers.Release</td>
<td>Release phone numbers back to inventory.</td>
</tr>
<tr>
<td>Phone numbers - View</td>
<td>PhoneNumbers.View</td>
<td>View a list of phone numbers that have been claimed or ported to your Amazon Connect instance.</td>
</tr>
<tr>
<td>Communication widget - Enable/Disable</td>
<td>ChatTestMode</td>
<td>Access a simulated web page so users can test the chat experience. Also grants them the permission to view a list of flows, which is exposed through the Test settings option.</td>
</tr>
<tr>
<td>Views</td>
<td>Views.View</td>
<td>Allow access to Views</td>
</tr>
</tbody>
</table>
## Users and permissions

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
</table>
| Users - Create   | Users.Create   | Add users to Amazon Connect. We recommend you limit who has these permissions. They pose a risk to your contact center because they can do the following:  
- Reset passwords, including that of the administrator.  
- Grant other users permission to the Admin security profile. People assigned to the Admin security profile have full access to your contact center.  
Doing these things would enable someone to lock out those who need to access Amazon Connect, and allow in others who can steal customer data |
<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users - Delete</td>
<td>Users.Delete</td>
<td>Delete users from Amazon Connect.</td>
</tr>
<tr>
<td>Users - Edit</td>
<td>Users.Edit</td>
<td>View and edit user records. As with Users - Create, limit who has these permissions because they pose a risk to your contact center.</td>
</tr>
<tr>
<td>Users - Edit permission</td>
<td>Users.EditPermission</td>
<td>View and edit user records. As with Users - Create, limit who has these permissions because they pose a risk to your contact center.</td>
</tr>
<tr>
<td>Users - View</td>
<td>Users.View</td>
<td>View user records.</td>
</tr>
<tr>
<td>Agent hierarchy - Create</td>
<td>AgentGrouping.CreateInstance</td>
<td>Create agent hierarchies. Add groups, teams, and agents.</td>
</tr>
<tr>
<td>Agent hierarchy - Edit</td>
<td>AgentGrouping&gt;Edit</td>
<td>Edit agent hierarchies.</td>
</tr>
<tr>
<td>Agent hierarchy - Enable/Disable</td>
<td>AgentGrouping.EnableAndDisable</td>
<td>View or edit agent hierarchy information.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent hierarchy - View</td>
<td>AgentGrouping.View</td>
<td>View the agent's hierarchy information in a real-time metrics report, which can include their location and skill set data.</td>
</tr>
<tr>
<td>Agent status - Create</td>
<td>AgentStates.Create</td>
<td>Create an custom agent status. The status appears in the Contact Control Panel (CCP), such as Break, Lunch, or Training.</td>
</tr>
<tr>
<td>Agent status - Edit</td>
<td>AgentStates.Edit</td>
<td>Edit a custom agent status.</td>
</tr>
<tr>
<td>Agent status - Enable/Disable</td>
<td>AgentStates.EnableAndDisable</td>
<td>View and edit custom agent states.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent status - View</td>
<td>AgentStates.View</td>
<td>View an agent's status in the real-time metrics report and historical metrics report. For example, if they are Available, Offline, or in a custom state. View their status in the Agent activity report.</td>
</tr>
</tbody>
</table>

**Contact Control Panel (CCP)**

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Contact Control Panel</td>
<td>BasicAgentAccess</td>
<td>Manages access to the Contact Control Panel (CCP). Assign this permission to agents as well as managers who need to monitor live conversations.</td>
</tr>
<tr>
<td>Contact Lens data</td>
<td>RealtimeContactLens.View</td>
<td>Enables users to view real-time analytics provided by Contact Lens.</td>
</tr>
<tr>
<td>Make outbound calls</td>
<td>OutboundCallAccess</td>
<td>Grants users permissions to make outbound calls. For more information about setting up outbound calling,</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voice ID</td>
<td>Voiceld.Access</td>
<td>Enables controls in the Contact Control Panel so agents can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View authentication outcomes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Opt-out or re-authenticate a caller.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update SpeakerID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View fraud detection results, rerun fraud analysis (fraud detection decision, fraud type and score).</td>
</tr>
<tr>
<td>Restrict task creation</td>
<td>RestrictTaskCreation.Access</td>
<td>Block agents from being able to create tasks.</td>
</tr>
<tr>
<td>Audio device settings</td>
<td>AudioDeviceSettings.Access</td>
<td>Choose your preferred device for speaker, microphone, and ringer in the Contact Control Panel (CCP) or agent workspace.</td>
</tr>
<tr>
<td>Video calls</td>
<td>VideoContact.Access</td>
<td>Enable agents to use video calling.</td>
</tr>
</tbody>
</table>
## Analytics and Optimization

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access metrics</td>
<td>AccessMetrics</td>
<td>Manage access to real-time and historical metrics reports.</td>
</tr>
<tr>
<td>Real-time metrics</td>
<td>AccessMetrics.RealTimeMetrics.Access</td>
<td>Manage access to the real-time metrics page.</td>
</tr>
<tr>
<td>Historical metrics</td>
<td>HistoricalMetrics.Access</td>
<td>Manage access to the historical metrics page.</td>
</tr>
<tr>
<td>Agent activity audit</td>
<td>AgentActivityAudit.Access</td>
<td>Manage access to the agent activity audit within the historical metrics page.</td>
</tr>
<tr>
<td>Contact Search</td>
<td>ContactSearch.View</td>
<td>Access the Contact search page, which is where users can search for contacts and see results on the Contact details page.</td>
</tr>
<tr>
<td>View My Contacts</td>
<td>MyContacts.View</td>
<td>Allows agents to view contacts that they themselves had handled, on Contact search and Contact details pages.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search contacts by conversation characteristics</td>
<td>ContactSearchWithCharacteristics.Access</td>
<td>Access to the Contact Lens filters that enable users to search by sentiment scores, non-talk time, and category.</td>
</tr>
<tr>
<td>Search contacts by conversation characteristics - View</td>
<td>ContactSearchWithCharacteristics.View</td>
<td>View the Contact Lens filters that enable users to search by sentiment scores, non-talk time, and category.</td>
</tr>
<tr>
<td>Search contacts by keywords</td>
<td>ContactSearchWithKeywords.Access</td>
<td>Search for contacts by keyword. On the Contact Search page, users can access additional filters that allow them to search Contact Lens transcripts by keywords or phrases, such as &quot;thank you for your business.&quot;</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search contacts by keywords - View</td>
<td>ContactSearchWithKeywords.View</td>
<td>Search for contacts by keyword. On the Contact Search page, users can access additional filters that allow them to search Contact Lens transcripts by keywords or phrases, such as &quot;thank you for your business.&quot;</td>
</tr>
<tr>
<td>Configure searchable contact attributes - View</td>
<td>ConfigureContactAttributes.View</td>
<td>Determine what custom attribute data will be searchable (by people who have the Contact attributes permission). It allows them to access the Searchable custom contact attributes page. For more information, see Search by custom contact attributes.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restrict contact access</td>
<td>ContactRecording.Access</td>
<td>If your organization isn't using Contact Lens for Amazon Connect, use this permission to manage who can listen to recordings, access the corresponding URLs that are generated in S3, and delete recordings. For more information, see Assign permissions to review recordings of past conversations. Checking this box limits a user's access to contacts based on their agent hierarchy. The user will only have access to contacts handled by agent within their own hierarchy.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restrict contact access</td>
<td>RestrictContactAccessByHierarchy.View</td>
<td>Manage a user's access to results on the Contact search page based on their agent hierarchy group. For more information, see <a href="#">Manage who can search for contacts and access detailed information</a>.</td>
</tr>
<tr>
<td>Contact attributes</td>
<td>ContactAttributes.View</td>
<td>View contact attributes. Also controls access to the search filters based on contact attributes. For more information, see <a href="#">Search by custom contact attributes</a>.</td>
</tr>
<tr>
<td>Contact Lens - conversational analytics - View</td>
<td>GraphTrends.View</td>
<td>On the Contact details page for a contact, users can view graphs that summarize conversational analytics, such as customer sentiment trend, sentiment, and talk time.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>-----</td>
</tr>
<tr>
<td>Contact Lens - custom vocabularies - Edit</td>
<td>ContactLensCustomVocabulary.Edit</td>
<td>Add custom vocabularies.</td>
</tr>
<tr>
<td>Contact Lens - custom vocabularies - View</td>
<td>ContactLensCustomVocabulary.View</td>
<td>Download and view custom vocabularies.</td>
</tr>
<tr>
<td>Contact Lens - post-contact summary</td>
<td>ContactLensPostContactSummary.View</td>
<td>View post-contact summarization powered by generative artificial intelligence (generative AI) on the Contact Search and Contact Details pages.</td>
</tr>
<tr>
<td>Contact Lens - theme detection - Create</td>
<td>ContactLensThemeDetection.Create</td>
<td>Create theme detection reports on the Contact search page.</td>
</tr>
<tr>
<td>Contact Lens - theme detection - View</td>
<td>ContactLensThemeDetection.View</td>
<td>View theme detection reports on the Contact search page.</td>
</tr>
<tr>
<td>Contact Lens - theme detection - Delete</td>
<td>ContactLensThemeDetection.Delete</td>
<td>Delete theme detection reports on the Contact search page.</td>
</tr>
<tr>
<td>Rules - Create</td>
<td>Rules.Create</td>
<td>Create rules.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recorded conversations (redacted)</td>
<td>RedactedData.View</td>
<td>On the <strong>Contact details</strong> and <strong>Contact search</strong> pages for a contact, listen to call recording files and view call transcripts in which the sensitive data has been removed.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recorded conversations (unredacted) - View</td>
<td>ListenCallRecordings</td>
<td>On the <strong>Contact details</strong> and <strong>Contact search</strong> pages for a contact, view unredacted content that contains sensitive data, such as name and credit card information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Original, unredacted chat transcripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Original, unredacted transcripts analyzed by Contact Lens</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Original, unredacted audio recordings</td>
</tr>
</tbody>
</table>

⚠️ **Important**  
If you have permissions to both **Recorded conversations (redacted)** and **Recorded conversations (unredacted)**, note the following behavior:
<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• By default only redacted recordings and transcripts are made available on the <strong>Contact details</strong> and <strong>Contact search</strong> pages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When no redacted content exists for the contact, or when redacted content cannot be shown to the user, then unredacted content is displayed on the <strong>Contact details</strong> and <strong>Contact search</strong> pages.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recorded conversations (unredacted) - Access</td>
<td>ListenCallRecordings</td>
<td>View the Play icon so they can listen to call recordings by using the Amazon Connect admin website.</td>
</tr>
</tbody>
</table>

To access unredacted conversations, remove permissions to `Recorded conversations (redacted)`. This leaves the user with only `Recorded conversations (unredacted)` permissions. You cannot access both the redacted and unredacted version of a conversation at the same time.
<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorded conversations (unredacted) - Enable download button</td>
<td>DownloadCallRecordings</td>
<td>Enables buttons to download and delete call recordings. By default, the Enable download button permission is granted so the user can download call recordings through the Amazon Connect admin website. To perform a download, however, the user needs permissions to access a Recorded conversation (unredacted).</td>
</tr>
<tr>
<td>Recorded conversations (unredacted) - Delete</td>
<td>DeleteCallRecordings</td>
<td>Delete call recordings. By default, the Enable download button permission is granted too so the user can delete recordings through the Amazon Connect admin website.</td>
</tr>
<tr>
<td>Login/Logout report - View</td>
<td>AgentTimeCard.View</td>
<td>View Login/Logout reports.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Real-time contact barge-in - Enable/Disable</td>
<td>ManagerBargeIn</td>
<td>Enables supervisors and managers to barge into live conversations between agents and customers. To learn more about Barge for live conversations, see <a href="#">Barge live conversations</a>.</td>
</tr>
<tr>
<td>Real-time contact monitoring- Enable/Disable</td>
<td>ManagerListenIn</td>
<td><strong>Monitor live conversations</strong> and listen to recordings of past conversations. Be sure to assign managers to the Agent security profile so they can access the Contact Control Panel (CCP). This enables them to monitor the conversation through the CCP.</td>
</tr>
<tr>
<td>Saved reports - View</td>
<td>MetricsReports.View</td>
<td><a href="#">View a shared report</a>.</td>
</tr>
<tr>
<td>Saved reports - Create</td>
<td>MetricsReports.Create</td>
<td><a href="#">Create and share reports</a>.</td>
</tr>
<tr>
<td>Saved reports - Edit</td>
<td>MetricsReports.Edit</td>
<td>Edit save reports.</td>
</tr>
<tr>
<td>Saved reports - Delete</td>
<td>MetricsReports.Delete</td>
<td>Delete saved reports.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Saved reports - Publish</td>
<td>MetricsReports.Publish</td>
<td>Publish reports.</td>
</tr>
<tr>
<td>Saved reports - Schedule</td>
<td>MetricsReports.Schedule</td>
<td><strong>Schedule a saved report.</strong> By default, the user gets permission to create, delete, edit, and view a saved report.</td>
</tr>
<tr>
<td></td>
<td>MetricsReports.Publish</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReportSchedules.Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReportSchedules.Delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReportSchedules.Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReportSchedules.View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluation.View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluation.Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evaluation.Delete</td>
<td></td>
</tr>
<tr>
<td>Evaluation forms - manage form definitions</td>
<td>EvaluationForms.Create</td>
<td>Create and manage evaluation forms.</td>
</tr>
<tr>
<td></td>
<td>EvaluationForms.View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EvaluationForms.Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EvaluationForms.Delete</td>
<td></td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voice ID - attributes and search</td>
<td>VoiceIdAttributesAndSearch.View</td>
<td>Search for and view Voice ID results on the <strong>Contact detail</strong> page.</td>
</tr>
<tr>
<td>Voice ID - attributes and search</td>
<td>VoiceIdAttributesAndSearch.View</td>
<td>Search for and view Voice ID results on the <strong>Contact detail</strong> page.</td>
</tr>
<tr>
<td>Forecasting - View</td>
<td>Forecasting.View</td>
<td><strong>Review contact volume and average handle time forecasts.</strong></td>
</tr>
<tr>
<td>Forecasting - Edit</td>
<td>Forecasting.Edit</td>
<td><strong>Create and edit contact volume and average handle time forecasts.</strong></td>
</tr>
<tr>
<td>Forecasting - Publish</td>
<td>Forecasting.Publish</td>
<td><strong>Publish a forecast.</strong></td>
</tr>
<tr>
<td>Capacity planning - View</td>
<td>Capacity.View</td>
<td><strong>Review capacity plan output.</strong></td>
</tr>
<tr>
<td>Capacity planning - Edit</td>
<td>Capacity.Edit</td>
<td><strong>Create capacity planning scenarios.</strong></td>
</tr>
<tr>
<td>Capacity planning - Publish</td>
<td>Capacity.Publish</td>
<td><strong>Publish a capacity plan.</strong></td>
</tr>
<tr>
<td>Forecast and schedule interval</td>
<td>Forecasting/Edit</td>
<td><strong>Set the forecast and schedule interval.</strong></td>
</tr>
<tr>
<td>Dashboards</td>
<td>AccessMetrics.Dashboards.Access</td>
<td><strong>Dashboards</strong></td>
</tr>
</tbody>
</table>

**Security profiles**
### Contact Actions

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer Contact</td>
<td>TransferContact.Enabled</td>
<td><strong>Transfer contacts on Analytics and optimization pages.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Currently transfer of task contacts to quick connects is supported on the <strong>Contact details</strong> page.</td>
</tr>
<tr>
<td>End contact</td>
<td>StopContact.Enabled</td>
<td><strong>End contacts on Analytics and optimization pages.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Currently supported on the <strong>Contact details</strong> page.</td>
</tr>
<tr>
<td>Reschedule contact</td>
<td>UpdateContactSchedule.Enabled</td>
<td><strong>Reschedule previously scheduled contact on Analytics and optimization pages.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Currently supported on the <strong>Contact details</strong> page for task contacts only.</td>
</tr>
</tbody>
</table>

### Historical changes

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>View historical changes</td>
<td>HistoricalChanges.View</td>
<td>On the <strong>User management</strong> page, view historical</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>changes to user records.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Customer Profiles**

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>CustomerProfiles.Create</td>
<td><a href="#">Create customer profiles in the agent application.</a></td>
</tr>
<tr>
<td>Edit</td>
<td>CustomerProfiles.Edit</td>
<td>Edit customer profiles in the agent application.</td>
</tr>
<tr>
<td>View</td>
<td>CustomerProfiles.View</td>
<td>View customer profiles in the agent application.</td>
</tr>
<tr>
<td>Created Attributes</td>
<td>CustomerProfiles.CalculatedAttributes.Create</td>
<td>Create calculated attributes.</td>
</tr>
<tr>
<td>Created Attributes</td>
<td>CustomerProfiles.CalculatedAttributes.Edit</td>
<td>Edit calculated attributes.</td>
</tr>
<tr>
<td>Created Attributes</td>
<td>CustomerProfiles.CalculatedAttributes.Delete</td>
<td>Delete calculated attributes.</td>
</tr>
<tr>
<td>Created Attributes</td>
<td>CustomerProfiles.CalculatedAttributes.View</td>
<td>View calculated attributes.</td>
</tr>
</tbody>
</table>

Security profiles
## Scheduling

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule manager - View</td>
<td>Scheduling.View</td>
<td>View generated staff schedules in the Schedule manager user experience.</td>
</tr>
<tr>
<td>Schedule manager - Edit</td>
<td>Scheduling.Edit</td>
<td>Create, edit schedule configuration and publish generated staff schedules.</td>
</tr>
<tr>
<td>Schedule manager - Publish</td>
<td>Scheduling.Publish</td>
<td>Publish a schedule by using Schedule Manager.</td>
</tr>
<tr>
<td>Published schedule calendar</td>
<td>Scheduling.View</td>
<td>View a schedule.</td>
</tr>
<tr>
<td>Team calendar</td>
<td>TeamCalendar.View</td>
<td>View published staff schedules in the Published Calendar user experience.</td>
</tr>
<tr>
<td>Team calendar</td>
<td>TeamCalendar.Edit</td>
<td>Edit published staff schedules in the Published Calendar user experience.</td>
</tr>
</tbody>
</table>

## Agent Applications

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent application schedule calendar</td>
<td>StaffCalendar.View</td>
<td>Ability for agents to view their schedules.</td>
</tr>
<tr>
<td></td>
<td>StaffCalendar.Edit</td>
<td></td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom views</td>
<td>CustomViews.Access</td>
<td>Use the <a href="#">Agent Workspace guided experience</a> guide.</td>
</tr>
<tr>
<td>Amazon Q in Connect</td>
<td>Wisdom.View</td>
<td><a href="#">View real-time recommendations</a> in the agent application.</td>
</tr>
<tr>
<td><code>&lt;p app name&gt;</code> - Access</td>
<td><code>&lt;p app name&gt;</code>.Access</td>
<td>Allows agents to access a third-party application.</td>
</tr>
<tr>
<td>Content Management - Quick responses - Create</td>
<td>ContentManagement.Create</td>
<td>Set up a <a href="#">knowledge base to store quick responses</a>. Create, import, and view the import history of quick responses that are displayed in the agent application.</td>
</tr>
<tr>
<td>Content Management - Quick responses - Edit</td>
<td>ContentManagement.Edit</td>
<td>Edit, import, and view the import history of quick responses that are displayed in the agent application.</td>
</tr>
<tr>
<td>Content Management - Quick responses - View</td>
<td>ContentManagement.View</td>
<td>View a list of quick responses in the Amazon Connect admin website.</td>
</tr>
<tr>
<td>Content Management - Quick responses - Delete</td>
<td>ContentManagement.Delete</td>
<td>Delete quick responses by using the Amazon Connect admin website.</td>
</tr>
</tbody>
</table>
## Cases

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases - Create</td>
<td>Cases.Create</td>
<td>Create cases in the agent application.</td>
</tr>
<tr>
<td>Cases - View</td>
<td>Cases.View</td>
<td>View cases in the agent application.</td>
</tr>
<tr>
<td>Cases - Edit</td>
<td>Cases/Edit</td>
<td>Edit cases in the agent application.</td>
</tr>
<tr>
<td>Case Fields - Create</td>
<td>CaseFields.Create</td>
<td>Create case fields.</td>
</tr>
<tr>
<td>Case Fields - View</td>
<td>CaseFields.View</td>
<td>View case fields.</td>
</tr>
<tr>
<td>Case Fields - Edit</td>
<td>CaseFields/Edit</td>
<td>Edit case fields.</td>
</tr>
<tr>
<td>Case Templates - Create</td>
<td>CaseTemplates.Create</td>
<td>Create case templates.</td>
</tr>
<tr>
<td>Case Templates - View</td>
<td>CaseTemplates.View</td>
<td>View case templates.</td>
</tr>
<tr>
<td>Case Templates - Edit</td>
<td>CaseTemplates/Edit</td>
<td>Edit case templates.</td>
</tr>
</tbody>
</table>

## Campaigns

<table>
<thead>
<tr>
<th>UI name</th>
<th>API name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campaigns - Create</td>
<td>Campaigns.Create</td>
<td>Create outbound campaigns.</td>
</tr>
<tr>
<td>Campaigns - Delete</td>
<td>Campaigns.Delete</td>
<td>Delete outbound campaigns.</td>
</tr>
<tr>
<td>Campaigns - Edit</td>
<td>Campaigns.Edit</td>
<td>Edit outbound campaigns.</td>
</tr>
<tr>
<td>UI name</td>
<td>API name</td>
<td>Use</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Campaigns - Manage</td>
<td>Campaigns.Delete</td>
<td>Manage outbound campaigns.</td>
</tr>
<tr>
<td>Campaigns - View</td>
<td></td>
<td>View outbound campaigns.</td>
</tr>
</tbody>
</table>

**Default security profiles**

Amazon Connect includes default security profiles for general roles. You can review the permissions granted by these profiles and use them if they align with the permissions that your users need. Otherwise, create a security profile that grants your users only the permissions they need.

The following table lists the default security profiles.

<table>
<thead>
<tr>
<th>Security profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Grants administrators permission to perform a majority of actions.</td>
</tr>
<tr>
<td>Agent</td>
<td>Grants agents permission to access the CCP.</td>
</tr>
<tr>
<td>CallCenterManager</td>
<td>Grants managers permission to perform actions related to user management, metrics, and routing.</td>
</tr>
<tr>
<td>QualityAnalyst</td>
<td>Grants analysts permission to perform actions related to metrics.</td>
</tr>
</tbody>
</table>

**Note**

New permissions are added on a regular basis. We recommend revisiting your permission configurations to ensure your users can access the latest Amazon Connect features.
Assign a security profile to a user

Required permissions to assign security profiles

Before you can assign a security profile to a user, you must be logged in with an Amazon Connect account that has the Users - Edit permission, as shown in the following image. Or, if you're creating the user's account for the first time, you need Users - Create permission.

By default, the Amazon Connect Admin security profile has these permissions.

How to assign security profiles

1. Review Best practices for security profiles.
2. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
3. Choose Users, User management.
4. Select one or more users and choose Edit.
5. For Security Profiles, add or remove security profiles as needed. To add a security profile, put your cursor in the field and select the security profile from the list. To remove a security profile, click the x next to its name.
6. Choose Save.

Create a security profile

Creating a security profile enables you to grant your users only the permissions that they need.

For each permission group, there is a set of resources and supported set of actions. For example, users are part of the Users and permissions group, which supports the following actions: view, edit, create, remove, enable/disable, and edit permission.
Some actions depend on other actions. When you choose an action that depends on another action, the dependent action is automatically chosen and must also be granted. For example, if you add permission to edit users, we also add permission to view users.

**Required permissions to create security profiles**

Before you can create a new security profile, you must be logged in with an Amazon Connect account that has **Security profiles - Create** permissions, as shown in the following image.

![Users and permissions](image)

By default, the Amazon Connect **Admin** security profile has these permissions.

**How to create security profiles**

1. Log in to the Amazon Connect admin website at `https://instance name.my.connect.aws/`
2. Choose **Users, Security profiles**.
3. Choose **Add new security profile**.
4. Type a name and description for the security profile.
5. Choose the appropriate permissions for the security profile from each permission group. For each permission type, choose one or more actions. Selecting some actions results in other actions being selected. For example, selecting **Edit** also selects **View** for the resource and any dependent resources.
6. Choose **Save**.

**Tag-based access controls**

You create a security profile with access control tags. Use these steps to create a security profile that enforces tag-based access controls.
1. Choose **Show advanced settings** at the bottom of the security profile.

2. In the **Access control** section, in the **Resources** box, enter the resources to be restricted using tags.

3. Enter the **Key** and **Value** combination for the resource tags that you want to restrict access to.

4. Ensure that you have enabled **View** permissions for the resources that you have selected.

5. Choose **Save**.

---

**Note**

It is mandatory to specify both a resource type and an access control tag when configuring tag based access controls. As a best practice, ensure that you have matching resource tags on a security profile that has tag based access controls configured. To learn more about tag based access controls in Amazon Connect, see [Tag-based access control](#).

---

**Tag security profiles**

You can create a new security profile with resource tags. Use these steps to add a resource tag to a security profile.

1. Choose **Show advanced settings** at the bottom of the security profile.

2. Enter a **Key** and **Value** combination to tag the resource, as shown in the following image.

3. Choose **Save**.
For more information about tagging resources, see Tagging resources in Amazon Connect.

Update security profiles

You can update a security profile at any time to add or remove permissions.

Required permissions to update security profiles

Before you can update permissions in a security profile, you must be logged in with an Amazon Connect account that has the following permissions: Security profiles - Edit.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Remove</th>
<th>Enable / Disable</th>
<th>Edit permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent hierarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By default, the Amazon Connect Admin security profile has these permissions.

How to update security profiles

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
   You must be logged in with an Amazon Connect account that has permissions to update security profiles.
3. Select the name of the profile.
4. Update the name, description, permissions, access control, and resource tags as needed.
5. Choose Save.

Note

Modifying the access control or resource tags on a security profile may impact the features or resources that a user with this security profile can access.
Tag-based access control

Tag-based access controls enable you to configure granular access to specific resources based on assigned resource tags. You can configure tag based access controls by using the API/SDK or within the Amazon Connect console (for supported resources).

Tag-based access control using the API/SDK

To use tags to control access to resources within your AWS accounts, you need to provide tag information in the condition element of an IAM policy. For example, to control access to your Voice ID domain based on the tags you've assigned to it, use the `aws:ResourceTag/key-name` condition key, along with a specific operator like `StringEquals` to specify which tag `key:value` pair must be attached to the domain, in order to allow given actions for it.

For more detailed information on tag-based access control, see [Controlling access to AWS resources using tags](#) in the IAM User Guide.

Tag-based access control using the Amazon Connect console

A `resource` tag is a custom metadata label that you can add to a resource in order to make it easier to identify, organize, and find in a search. You can apply tags programmatically using the Amazon Connect SDK/APIs, and for certain resources you can apply tags from within the Amazon Connect console. To learn more about resource tags, see [Tagging resources in Amazon Connect](#).

An access control tag is similar to a resource tag in that it uses the same `Key:value` structure. However, the distinction with an access control tag is that it introduces authorization controls that limit a user's access, to only specified resources containing resource tags with identical `Key:value` pairs. Access control tags are defined within security profiles, by first selecting the resource (routing profile, queue, users, etc.) for which to control access to, and then defining the `Key:value` pair to match on. Once a security profile with access control tags has been applied to a user, it will limit the user's access based on the defined combination of the selected resource(s) and access control tag(s) (`Key:value`). Without access control tags applied, a user will be able to see all resources if given permission to do so.

To use tags to control access to resources within the admin website of your Amazon Connect instance, you need to configure the access control section within a given security profile. For example, to control access to a routing profile based on the tags you've assigned to it, you would specify the routing profile as an access controlled resource, and then specify which tag `Key:value` pair you would like to enable access to.
Configuration limitations

Access control tags are configured on a security profile. You can configure up to four access control tags on a single security profile. Adding additional access control tags will make that security profile more restrictive. For example, if you were to add two access control tags like Department:X and Country:Y, the user would only be able to see resources containing both tags.

Users can be assigned a maximum of two security profiles that contain access control tags. When multiple security profiles containing access control tags are assigned to a single user, the tag based access controls become less restrictive. For example, if a user had one security profile with an access control tag like Country:USA, and another security profile with an access control tag like Country:Argentina, a user would be able to see resources tagged with Country:USA or Country:Argentina. A user can have other security profiles, as long as those additional security profiles do not contain tags. In the scenario where multiple security profiles are present with overlapping resource permissions, the security profile without tag based access controls will be enforced over the one with tag based access controls.

Service linked roles are required in order to configure resource tags or access control tags. If your instance was created after October 2018, this will be available by default with your Amazon Connect instance. However if you have an older instance, please refer to Use service-linked roles for Amazon Connect for instructions for how to enable service linked roles.

Amazon Connect tagging best practices

Applying tag based access controls is an advanced configuration feature that is supported by Amazon Connect and that follows the AWS shared responsibility model. It is important to ensure that you are correctly configuring your instance to comply with your desired authorization needs. For more information, please review the AWS shared responsibilities model.

Ensure that you have enabled at least view permissions for the resources that you enable tag based access control for. This will ensure that you avoid permission inconsistencies that result in denied access requests.

Tag based access controls are enabled at the resource level, which means that each resource can be restricted independently. In certain use cases this may be acceptable but it is considered best practice to enable tag based access controls to all resources together. For example, enabling access to users but not security profiles, would allow a user to create a security profile with privileges that supersede your intended user access control settings.
When logged in to the Amazon Connect console with tag based access controls applied, users will not be able to access historical change logs for the resources that they are restricted on.

As a best practice, you should disable access to the following resources/modules when applying tag based access controls within the Amazon Connect console. If you do not disable access to these resources, users with tag based access controls on a particular resource that view these pages may see an unrestricted list of users, security profiles, routing profiles, or queues. For more information on how to manage permissions, see [List of security profile permissions](#).

<table>
<thead>
<tr>
<th>Modules</th>
<th>Permission to disable access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact search</td>
<td>Contact Search</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Access metrics</td>
</tr>
<tr>
<td>Flow/Flow module</td>
<td>Flow modules - View</td>
</tr>
<tr>
<td>Forecasting</td>
<td>Forecasting</td>
</tr>
<tr>
<td>Historical changes/Audit portal</td>
<td>Access metrics</td>
</tr>
<tr>
<td>Historical metrics</td>
<td>Historical metrics</td>
</tr>
<tr>
<td>Login/Login out report</td>
<td>Login/Logout report - View</td>
</tr>
<tr>
<td>Outbound Campaign</td>
<td>Campaigns - View</td>
</tr>
<tr>
<td>Quick connect</td>
<td>Quick connects - View</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules - View</td>
</tr>
<tr>
<td>Saved reports</td>
<td>Saved reports - View</td>
</tr>
<tr>
<td>Scheduling</td>
<td>Schedule manager</td>
</tr>
<tr>
<td>Scheduling</td>
<td>Published schedule calendar</td>
</tr>
</tbody>
</table>
Set up routing

In Amazon Connect, routing consists of three parts: queues, routing profiles, and flows. This topic discusses queues and routing profiles. For information about flows, see Create Amazon Connect Flows.

A queue holds contacts waiting to be answered by agents. You can use a single queue to handle all incoming contacts, or you can set up multiple queues.

Queues are linked to agents through a routing profile. When you create a routing profile, you specify:

- Which queues will be in it.
- Whether one queue should be prioritized over another.
- What channels agents will handle in the Contact Control Panel (CCP).
- How many contacts agents can handle simultaneously for each channel.
- Whether individual queues are for all channels or specific ones.

Each agent is assigned to one routing profile.

Contents

- How routing works
- Create a queue
- Disable a queue
- Delete a queue
- Set the Maximum contacts in queue limit
- Set the hours of operation and timezone for a queue
- Create a routing profile
- Delete a routing profile
- Set up queue-based (skills-based) routing

How routing works

Contacts are routed through your contact center based on these factors:
• The routing profile an agent is assigned to.
• The hours of operation for a given queue.
• The routing logic you define in your flows.

For example, you use routing profiles to route specific types of contacts to agents with specific skill sets. If no agent with the required skill set is available, you can place the contact in the queue defined in the flow.

Here's the logic Amazon Connect uses to route contacts:

• Contacts in a queue are automatically prioritized and forwarded to the next available agent (that is, the agent who has been idle longest).

• Contacts are placed on hold if there are no available agents. The order in which they are serviced is determined by their time in queue, on a first-come, first-served basis.

• If multiple agents are ready for a contact, by default an inbound contact is routed to the agent who has been in the Available status for the longest time.

Handling either inbound or outbound contacts causes agents to drop to the bottom of the list for inbound contacts. You can set up your routing profile to ignore outbound contacts in this calculation by choosing the Outbound calls should not impact routing order option. Consider choosing this option if your organization wants agents to take outbound calls and still get a fair share of inbound contacts.

For example:

• Joe is third in line for inbound contacts, which are preferable to outbound contacts because he knows he will speak to someone, and that increases his odds of getting recognition in his role. Because he is idle, Joe decides to make an outbound contact to chip away at the backlog. He may or may not reach someone.

• By default, when Joe makes the outbound contact, he moves from third in line to the bottom of the list of agents waiting to receive an inbound contact. (If there are 10 agents, he is moved to 10th place). If instead he should remain in third place, you can override the default behavior.

• A routing profile may assign a priority to one queue over another, but the priority within the queue is always set by the order the contact was added to the queue.
How routing works with multiple channels

When you set up a routing profile to handle multiple channels, you must specify whether agents can handle contacts while already on another channel. This is called cross-channel concurrency. When using cross-channel concurrency, Amazon Connect checks which contact to offer the agent as follows:

1. It checks what contacts/channels the agent is currently handling.
2. Based on what channels they are currently handling, and the cross-channel configuration in the agent's routing profile, it determines whether the agent can be routed the next contact.

For a detailed example of how Amazon Connect routes contacts when cross-channel concurrency is set up, see Example of how a contact is routed with cross-channel concurrency.

Learn more about routing

See the following topics to learn more about routing:

- Concepts: Routing profiles
- Concepts: Queue-based routing
- Set up queue-based routing

Create a queue

This topic explains how to create a queue using the Amazon Connect console. To create queues programmatically, see the create-queue AWS CLI or CreateQueue in the Amazon Connect API Reference.

How many queues can I create? To view your quota of Queues per instance, open the Service Quotas console at https://console.aws.amazon.com/servicequotas/.

To create a queue

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/..
   Use an Admin account, or an account that has Routing - Create queues security profile permissions.
2. In Amazon Connect, on the navigation menu, choose Routing, Queues, Add new queue.
3. Add the appropriate information about your queue and choose **Add new queue**.

See the following topics for detailed information about each of the above areas:

1. **Set the hours of operation and timezone for a queue**
2. **Set up outbound caller ID**
3. **Set the Maximum contacts in queue limit**
4. **Create quick connects**

The queue is automatically active.
4. Assign the queue to a routing profile; for information, see Create a routing profile. The routing profile links the queue and agents together.

5. Add Tags to identify, organize, search for, filter and control who can access this queue. For more information, see Tagging resources in Amazon Connect.

To learn how queues work, see Concepts: Routing profiles and Concepts: Queue-based routing.

Disable a queue

You can quickly control the flow of contacts to queues by temporarily disabling a queue. When a queue is disabled, it's put in an offline mode. No new contacts are routed to the queue, but any existing contacts already in the queue are routed to agents.

Only users who have a security profile with Queues - Enable/Disable permissions can disable a queue.

To disable an active queue

1. On the navigation menu, choose Routing, Queues.
2. Hover over the name of the queue to edit. Choose the power icon that appears.
3. Choose **Disable** to confirm you want to disable the queue. You can immediately re-enable the queue if needed by choosing the power button again.

## Delete a queue

To delete a queue from your Amazon Connect instance, use the **DeleteQueue** API or the **delete-queue** AWS CLI.

It isn't possible to delete a queue by using the Amazon Connect admin website.

## Set the Maximum contacts in queue limit

By default a queue can contain up to your **service quota** for voice, chat, and tasks:

- **Concurrent active calls per instance**
- **Concurrent active chats per instance (includes SMS)**
- **Concurrent active tasks per instance**

To increase one of these quotas, you must request a quota increase. For more information, see **Amazon Connect service quotas**.

There may be situations where you want a specific queue to allow fewer contacts than the allowed quota. For example:
• You have a queue that is dedicated to calls about complicated issues that take an average of 15 minutes to resolve, you may want to limit the number of calls allowed in the queue to be less than **Concurrent active calls per instance**. This prevents customers from waiting for hours.

• You may have a queue dedicated to chats. Your service limit is 100 but you want only up to 20 chats at a time. You can set that value so Amazon Connect limits the number of active chats routed to that queue.

• You have a queue that combines more than one channel, and you set a custom value. Note that the queue stops accepting new contacts after that number is reached, regardless of the distribution of contacts. For example, if you set the value to 50, and the first 50 contacts are chats, then voice calls are not routed to this queue.

This topic explains how to reduce the allowed number of contacts in a queue for these situations.

**Reduce the number of contacts allowed in a queue**

To reduce the number of contacts allowed in a **standard queue** at the same time, you set the **Maximum contacts in queue** limit for the standard queue. This setting does not apply to **agent queues**; those are always limited to 10 contacts.

When you enter a number in **Maximum contacts in queue**, Amazon Connect validates that the number is less than the sum of your concurrent active contacts service quotas: **Concurrent calls per instance + Concurrent active chats per instance + Concurrent active tasks per instance**.

**Important**

- You must set **Maximum contacts in queue** to be less than the sum of the following quotas combined: **Concurrent calls per instance + Concurrent active chats per instance + Concurrent active tasks per instance**.
- Incoming calls and queued callbacks count towards the queue size limit.
For information about default service quotas and how to request an increase, see Amazon Connect service quotas.

To reduce the number of contacts allowed in a specific queue

1. On the navigation menu, choose Routing, Queues, Add new queue. Or, edit an existing queue.
2. In Maximum contacts in queue, choose Set a limit across all channels. If the queue is also used for chats or tasks, then all three channels will be capped at the same maximum.
3. In the box, specify how many contacts can be in the queue before it's considered full. The value cannot exceed the sum of Concurrent active calls per instance + Concurrent active chats per instance + Concurrent active tasks per instance.

<table>
<thead>
<tr>
<th>Maximum contacts in queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the maximum contacts allowed to be in the queue at the same time. This defines the routing decisions when a queue is full.</td>
</tr>
<tr>
<td>Set a limit across all channels</td>
</tr>
<tr>
<td>Maximum contacts in queue</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>Required</td>
</tr>
</tbody>
</table>

What happens to calls when a queue is full

- Incoming calls: The next incoming call gets a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.
- Queued callbacks: The next queued callback is routed down the error branch.

What happens if Maximum contacts in queue is set to 0

If you set Maximum contacts in queue to 0 it renders the queue unusable. The behavior is the same as when a queue is full.

Queue maximum limit exceptions

There are times when you can add more contacts to a queue than the set Maximum contacts in queue limit.
• There may be a slight delay between the time that a queue reaches its capacity limit and when this limit is enforced in the flow. This delay could cause incoming contacts to be queued during that time, particularly during bursts of traffic.

Additionally, Amazon Connect includes a 20 percent buffer to the queue capacity for the following exceptional scenarios:

• A contact was transformed into a Queued Callback, scheduled to be added to the queue at X time using the Initial delay setting in the flow. However, when the scheduled time arrived, the target queue had reached its Maximum capacity in queue limit. In this scenario, Amazon Connect allows the Queued Callback to be enqueued up to a 20 percent buffer of the Maximum capacity in queue limit for the queue.

• A contact, previously queued in Queue1, is now being transferred to Queue2 through the flow. However, when the transfer is attempted, Queue2 has already reached its Maximum capacity in queue limit. In this scenario, Amazon Connect allows the transfer to proceed, up to a 20 percent buffer of the Maximum capacity in queue limit for Queue2.

• An agent initiates a manual transfer of a contact into a queue through quick connects. However, when the transfer is attempted, the queue has already reached its Maximum capacity in queue limit. In this scenario, Amazon Connect allows the transfer to proceed, up to a 20 percent buffer of the Maximum capacity in queue limit.

Route contacts based on queue capacity

To define routing decisions based on queue capacity, use a Transfer to queue block to check whether a queue is full (Maximum contacts in queue), and then route the contact accordingly.

The Transfer to queue block checks the Maximum contacts in queue. If no limit is set, the queue is limited to the number of total concurrent contacts for the following quotas:

• Active tasks per instance
• Concurrent calls per instance
• Concurrent chats per instance
Set the hours of operation and timezone for a queue

The first thing you need to do when you set up a queue is to specify the hours of operation and timezone. The hours may be referenced in flows. For example, when routing contacts to agents, you might use the Check hours of operation block first, and then route the contact to the appropriate queue.

How many hours of operation can I create? To view your quota of Hours of operation per instance, open the Service Quotas console at https://console.aws.amazon.com/servicequotas/.

To set the hours of operation and timezone for a queue

1. On the navigation menu, choose Routing, Hours of operation.
2. To create a template, choose Add new hours and enter a name and a description.
3. For Time zone, select a value.
4. For Add new, set new hours.
5. Choose Save.
6. Now you can specify these the hours of operation when you create a queue, and check them in the Check hours of operation block.

How to specify midnight

To specify midnight, enter 12:00AM.

For example, if you want to set your hours to 10:00AM to midnight, you would enter: 10:00AM to 12:00AM. Your call center would be open for 14 hours. Here's the math:

- 10:00AM-12:00PM = 2 hours
- 12:00PM-12:00AM = 12 hours
- Total = 14 hours

Examples

Schedule for 24x7
Schedule for Monday to Friday 9:00 AM to 5:00 PM

Remove Sunday and Saturday from the schedule.

The final schedule looks like this:

Add lunch and other breaks

If your entire contact center were to close for lunch from 12-1, for example, then you'd enter hours to specify that, as in the following image:
In most contact centers breaks are staggered. While some agents are at lunch, for example, others are still available to handle contacts. Instead of specifying this in the hours of operation, you add custom agent statuses that appear in the agent's Contact Control Panel (CCP).

For example, you might create a custom status named Lunch. When the agent goes to lunch, they change their status in the CCP from Available to Lunch. During this time, no contacts are routed to them. When they return from lunch and are ready to take contacts again, they change their status back to Available.

Supervisors can change an agent's status using the real-time metrics report.

For more information, see these topics:

- Add custom agent status
- About agent status
- Change the "Agent activity" status in a real-time metrics report

**What happens during daylight saving time**

Amazon Connect uses the timezone to determine whether daylight saving time is in effect for the queues, and adjusts automatically for all timezones that observe daylight saving time. When a contact comes in, Amazon Connect looks at the hours and timezone to determine whether the contact can be routed to the given queue.

⚠️ **Important**

Amazon Connect provides options for EST5EDT, PST8PDT, CST6CDT, and more. For example, EST5EDT is defined as:

- **Eastern Standard Time (EST)** is used when observing standard time. It is five hours behind Coordinated Universal Time (UTC).
- **Eastern Daylight Time (EDT)** is used when observing daylight saving time. It is four hours behind Coordinated Universal Time (UTC).
We recommend researching your choice of timezone to ensure you understand it.

Use the Check Hours of Operation block

At the start of your flows, use the Check hours of operation block to determine whether your contact center is open, and to branch accordingly.

Create a routing profile

While queues are a 'waiting area' for contacts, a routing profile links queues to agents. When you create a routing profile, you specify:

- Channels: Which channels—voice, chat, task—are routed to this group of agents; whether to allow channels concurrently.
- Queues: Which queues are in the routing profile; whether one queue should be prioritized over another.

Each agent is assigned to one routing profile. For more information about routing profiles and queues, see Concepts: Routing profiles.

How many routing profiles can I create? To view your quota of Routing profiles per instance, open the Service Quotas console at https://console.aws.amazon.com/servicequotas/.

To create a routing profile

2. In the Routing Profile Details section, in the Name box, enter a searchable display name. In the Description box, enter what the profile is used for.
3. In the Channel Settings section, enter or choose the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel availability</td>
<td>Choose which types of contacts will be routed to agents who are assigned to this routing profile.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum contacts per agent</td>
<td>For chat and task channels, specify how many contacts that an agent can handle simultaneously, up to 10.</td>
</tr>
<tr>
<td>Cross-channel concurrency</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No other channels while agent is on channel. For example, while an agent is on a chat, they will not receive a voice contact or a task.</td>
</tr>
<tr>
<td></td>
<td>• Allow other channel concurrently. For example, while an agent is on a voice contact, they can be offered contacts from any other channels enabled in the routing profile, such as chats and tasks.</td>
</tr>
</tbody>
</table>

See [Example of how a contact is routed with cross-channel concurrency](#).

4. In the Queues section, enter the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Use the dropdown menu or text field to choose a queue that you've already</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Channels</strong></td>
<td>Choose whether the queue is for chat, voice, task, or all three.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>The channel that you specify here must also be specified in the Channel Settings section. If it isn't, contacts from that channel won't be routed to agents.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Specify the order in which contacts are to be handled for that queue. For example, a contact in a queue with a priority of 2 would be a lower priority than a contact in a queue with a priority of 1.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delay (in seconds)</td>
<td>Enter the minimum amount of time a contact should be in the queue before they are routed to an available agent. To learn more about how Priority and Delay work together, see Concepts: Queues priority and delay.</td>
</tr>
<tr>
<td>Default outbound queue</td>
<td>Choose a queue to be associated with outbound calls placed by the agents.</td>
</tr>
<tr>
<td>Set routing order</td>
<td>By default Amazon Connect routes new contacts to agents that have been in Available status the longest. You can customize this behavior, for example, to change the impact that outbound contacts have on the assignment of new inbound contacts.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound calls should not impact routing order</td>
<td>Use this setting if you don’t want agents who make outbound contacts to move to the bottom of the list for receiving inbound contacts. By default new contacts are routed to the agent who has been in Available status longest. By making an outbound contact, the agent drops to the bottom of the list waiting for inbound contacts. You can use this setting to override that default logic and ensure that agents making outbound contacts still get their fair share of inbound contacts.</td>
</tr>
</tbody>
</table>

5. In the Tags section, add tags to manage who can access routing profiles.

6. Choose Save.

**Tips for setting up channels and concurrency**

- Use Channel availability to toggle on and off whether agents assigned to a profile get voice, chat, and task contacts.

  For example, there are 20 queues assigned to a profile. All of the queues are enabled for voice, chat, and task. By removing the Voice option at the routing profile level, you can stop all voice calls to these agents, across all queues in the profile. When you want to restart voice contacts for these agents again, select Voice.

- When using Cross-channel concurrency, Amazon Connect checks which contact to offer the agent as follows:
1. It checks what contacts/channels the agent is currently handling.

2. Based on what channels they are currently handling, and the cross-channel configuration in the agent's routing profile, it determines whether the agent can be routed the next contact.

3. Amazon Connect prioritizes the longest waiting contact if Priority and Delay are equal. Even though it's evaluating multiple channels at the same time, First-In First-Out is still respected.

See [Example of how a contact is routed with cross-channel concurrency](#).

- For each queue in the profile, choose whether it's for voice, chat, task, or all three.

- If you want a queue to handle voice, chat, and task, but want to assign a different priority to each channel, add the queue twice. For example, in the following image, voice is priority 1 but chat and task are priority 2.

![Example of how a contact is routed with cross-channel concurrency](#)

**Example of how a contact is routed with cross-channel concurrency**

For example, assume an agent is assigned to the routing profile that has the channel settings shown in the following image. They can be routed voice, chat, and task contacts. They can receive cross-channel contacts when on tasks.

![Channel Settings](#)

The agent will experience the following routing behavior:
1. Assume the agent is fully idle. Next, the agent accepts a chat and begins working on it. Meanwhile, a task comes into queue.
   • Chat is set to No other channels allowed.
   • So even though there is a task in queue, it will not be offered to this agent.

2. Next, there is a chat in queue.
   • The agent's maximum chat concurrency is 2, so they are routed another chat for total of 2 chats. The agent continues working on both of the chats.

3. There are no other chats in queue. The agent finishes both chats (closes ACW).
   • There is still a task waiting in queue.
   • At this point, the task is offered to the agent because they are fully idle again. The agent begins working the task.

4. Another chat comes into queue.
   • Tasks is set to Allow other channels concurrently. So, even though the agent is already working on a task, they can still be offered the chat.
   • The chat gets routed to the agent, who now works on both the 1 chat and 1 task concurrently.

5. Now there is a Voice call in queue.
   • The agent is still working on 1 chat and 1 task.
   • Even though Task is set to Allow other channels concurrently, the agent is still working on 1 chat, and Chat is set to No other channels while agent is on a Chat contact. So, the voice call is not routed to the agent. The agent continues working on both the chat and the task.

6. The agent completes the chat, but still works on the task.
   • Now, because the only contact still assigned to the agent is a task, and Tasks are set to Allow other channels concurrently, this means that the agent can be offered the voice call.
   • The agent picks up the voice call and is now working concurrently on both the voice call and the task.

7. Now there is another task in queue.
   • The agent is currently working on a voice call AND a task. Once again, Amazon Connect checks the cross channel settings and Voice is set to No other channels while agent is on a Voice contact.
   • Because the agent is working on a voice call, they cannot be offered any tasks until they are done with the voice call.
Also, because **Task** is set to **Maximum contacts per agent** is 1, even after the agent handles the voice call, they still won't be offered the task until they finish their current task.

## Delete a routing profile

To delete a routing profile from your Amazon Connect instance, use the `DeleteRoutingProfile` API or the `delete-routing-profile` AWS CLI.

It isn’t possible to delete a routing profile by using the Amazon Connect admin website.

## Set up queue-based (skills-based) routing

Here's an overview of the steps to set up queue-based routing:

- **Create the queues**, for example, one for each skill you want to use for routing.
- **Create the routing profiles**:
  - Specify the channels supported by this routing profile.
  - Specify the queues: the channel, priority, and delay.
- **Configure agent settings** to assign the routing profiles to them.

When you **create your flows**, you'll add the queues to them. If a contact chooses to speak to an agent in Spanish, for example, they will be routed to the Spanish Reservations queue.

For information about how routing works, and queue-based routing, see these topics:

- **How routing works with multiple channels**
- **Concepts: Queue-based routing**

## Set up agents

You can manage and load-balance customer contacts using agent hierarchy organization and agent status management. These tools provide filtering and agent availability management per queue, skill set, and routing profiles.

**Contents**

- **Set up agent hierarchies**
Set up agent hierarchies

Agent hierarchies are a way for you to organize agents into teams and groups for reporting purposes. It's useful to organize them based on their location and their skill sets. For example, you might want to create large groups, such as all agents who work on a specific continent, or smaller groups such as all agents working in a specific department.

You can also configure hierarchies with up to five levels, and segment agents or teams. Here are a couple of things to note about using hierarchies:

- Removing agents from a level affects historical reporting.
- When you use the **Restrict contact access** permission, you can restrict contact search results based on the agent's hierarchy. For more information, see Manage who can search for contacts and access detailed information.

Required permissions

To create agent hierarchies, you need the **View - Agent hierarchy** permission in your security profile.

Note

Since agent hierarchies may include location and skill set data, you also need this permission to view the agent hierarchy information in a real-time metrics report.

The following image shows the **Users and permissions - Agent hierarchy** permissions on the Security profile permissions page.
Create a new agent hierarchy

**How many hierarchy groups can I create?** To view your quota of User hierarchy groups per instance, open the Service Quotas console at [https://console.aws.amazon.com/servicequotas/](https://console.aws.amazon.com/servicequotas/).

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create agent hierarchies.
2. Choose Users, Agent hierarchy.
3. Enter a name and choose + to create the first level of your hierarchy.
4. Choose + to add more levels to your hierarchy.
5. Choose Save to apply the changes, or Cancel to undo them.

**Tip**

If the Save button isn't active, you don't have permissions to create or edit the agent hierarchy.

Add groups, teams, and agents to a hierarchy

After you create a hierarchy, you can add groups, teams, and agents from the top down.

1. Select the top level of the hierarchy.
2. Choose x to add groupings to each level.
3. Choose the check icon to save the name, choose the pencil icon to edit the name.
4. Choose Save.
Choose **View historical changes** to view the change history. You can filter changes by date (between two dates) or by user name. If you cannot see the link, ensure that you have the proper permissions to view these changes.

### Delete an agent hierarchy

⚠️ **Important**

Deleting a hierarchy level severs the link to existing contacts. This action can not be reversed.

### Add custom agent status

Agents are responsible for setting their status in the Contact Control Panel (CCP). In fact, the only time an agent's status changes is when they manually change it in the CCP, or when their supervisor changes it in a real-time metrics report.

Amazon Connect provides two default status values:

- Available
- Offline

You can change the name of these values, and you can add new ones. For example, you might add a status for Lunch, and another for Training. These and the default status values will be used for reporting, metrics, and resource management.

When you add a new status, it will always be **Custom**, not routable.

You can't delete a status value but you can disable it so it doesn't appear on the agent's CCP.

**To add a new agent status**

1. Choose **Users, Agent status, Add new agent status**.
2. Enter a status name and description, and select whether the status should appear in the CCP to the agent.
3. Choose **Save**.
To change the order that the status values appear in the CCP, click the waffle next to the status value, as shown in the following image. Drag it to the order you want.

![Status values in CCP](image)

**To edit a status**

1. Choose **Users, Agent status**.
2. Hover over the status name and choose the edit icon.
3. Enter the new information, and choose **Save** to apply the changes.

Choose **View Historical Changes** to view the change history. You can filter changes by date (between two dates) or by user name. If you can't see the **View historical changes** link, make sure you have permissions to view these changes.

**Configure agent settings: routing profile, phone type, and auto-accept calls**

Before you configure your agent settings, here is some info to have on hand. Of course, you can always change this information later.

- What is their routing profile? They can only be assigned one.
- Will they have the **Agent** security profile or a custom profile you created?
- Are they going to use a soft phone? If so, will they be connected to contacts automatically, or will they need to press the **Accept** button in their Contact Control Panel (CCP)?
- Or, are they going to use a desk phone? If so, what is their number?
- How many seconds do they have for After contact work (ACW)? There's no way you can turn off ACW time altogether so agents never go to ACW. (A value of **0** means an indefinite amount of time.)
- Are they going to be assigned to an agent hierarchy?
Note
You can't configure how long an available agent has to connect with a contact before it's missed. Agents have 20 seconds to accept or reject a voice or chat contact, and 30 seconds for a task contact. If no action is taken, the current agent's status will be Missed and the contact is routed to the next available agent.

To configure agent settings
1. On the left navigation menu, go to Users, User management.
2. Choose the user you want to configure, then choose Edit.
3. Assign a routing profile to them. You can only assign one.
4. Assign the Agent security profile, unless you've created custom security profiles.
5. Under Phone Type choose whether the agent is using a desk phone or soft phone.
   - If you select desk phone, enter their phone number.
   - If you select soft phone, choose Auto-Accept Call if you want agents to be connected to calls automatically. This doesn't apply to chats.
6. In After call work (ACW) timeout, type how many seconds agents have for after contact work, such as entering notes about the contact.
   - Minimum setting is 1 second.
   - Maximum setting is 2,000,000 seconds (24 days).
   - Enter 0 if you don't want to allocate a specific amount of ACW time. It essentially means an indefinite amount of time. When the conversation ends, ACW starts; the agent must choose Close contact to end ACW.

The following image shows the Settings section of the Edit routing profile page. After call work (ACW) timeout set to 0.
7. Under **Agent Hierarchy** select any groups the agent should be part of.

8. Under **Tags**, add resource tags to identify, organize, search for, filter and control who can access this user.

## Enable auto-accept call for agents

When Auto-Accept Call is enabled for an available agent, the agent connects to contacts automatically.

### How long until the call is connected to the agent?

Less than one second. When a call arrives to an available agent who has Auto-Accept Call enabled, the Contact Control Panel (CCP) briefly shows the options **Accept** or **Reject**. This is expected behavior. After less than a second, the call is automatically accepted and these options disappear.

There isn’t an option for increasing the amount of time before a call is automatically accepted.

Auto-Accept Call doesn’t work for callbacks.

## Enable auto-accept call for existing agents

You can’t enable Auto-Accept Call while editing multiple existing users in your Amazon Connect instance. You must edit existing users individually to enable it. However, you can configure the setting for multiple new users when you bulk upload new users with the CSV template.

To complete these steps, you must log in as a user who has the following permissions in their security profile: **Edit, Create, Remove, Enable / Disable, and Edit** permission.
1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create or edit users.
2. On the left navigation menu, choose Users, User management.
3. In the list of users, select an agent, and then choose Edit.
4. On the Edit users page, under Phone Type, select the Auto-Accept Call check box.
5. Choose Save.
6. Repeat these steps for each user that you want to edit.

**Bulk upload new users with auto-accept call enabled**

You can't use the CSV template to edit information for existing users. If you include duplicate users with different information in the CSV template, you will receive an error.

1. Log in to your Amazon Connect instance using your access URL (https://domain.awsapps.com/connect/login).
2. On the left navigation menu, choose Users, User management.
3. Choose Add new users.
4. Under How do you want to set up your existing users?, next to Upload my users from a template (csv), choose template to download a pre-formatted CSV file.
5. In the CSV file, configure the details for the new users who you want to add. For soft phone auto accept (yes/no), be sure to enter yes.
6. After configuring the CSV file, in your Amazon Connect instance, choose Upload my users from a template (csv), and then choose Next.
7. Under Select and upload a spreadsheet with user details, choose Choose file.
8. Choose the configured CSV file from its location on your computer.
9. In your Amazon Connect instance, choose Upload and verify.
10. Under Verify user details, verify that the information is correct for the new users, and then choose Create users.

**(Optional) Verify the change in CCP logs**

To confirm that Auto-Accept Call is enabled for an agent, download the CCP logs generated for that agent: in the CCP for the agent, choose Settings, Download logs. The logs are saved to your browser's default download directory.
In the logs, the `autoAccept` attribute is set to "true" if this setting is enabled. The logs show something like this:

```
"type": "agent",
"initial": false,
"softphoneMediaInfo": {
    "callType": "audio_only",
    "autoAccept": true
}
```

**CCPv1: Log out agents automatically when they close their CCP**

⚠️ **Important**

This topic only applies to customers who use CCPv1. The URL for CCPv1 ends with `/ccp#`

When using the default Amazon Connect CCPv1, closing the CCP window or logging out doesn't automatically change an agent's status from **Available** to **Offline**. An agent must change their status manually to **Offline** and then log out.

To change this behavior, you can do one of the following:

- Use CCPv2. When agents log out, their status is automatically switched to **Offline**. However, note that CCPv2 doesn't automatically switch agents to **Offline** if they only close the window. For instructions on upgrading to CCPv2, see **My CCP URL ends with /ccp#**.
- Use the [CreateAgentStatus](#) API: You can change the state of the agent to **Offline**.
- Create a custom CCP. See [Amazon Connect Streams API](#) and the [Agent API](#)
- Use the following steps in this topic to update your CCP so it switches agents to **Offline** and logs out agents automatically when they close the CCP window.

**Step 1: Set up the Streams API**

For instructions, see the [Amazon Connect Streams Documentation](#).

**Step 2: Update your application code to change the agent state**

Integrate the following Streams API calls into your web application:
1. Use `connect.agent()` to subscribe to agent events and retrieve agent objects.

```javascript
let mAgent;

connect.agent(function(agent) {
  mAgent = agent;
});
```

2. Call `agent.setState()` in the onbeforeunload event handler to change the agent state. The agent is marked Offline after executing the beforeunload function.

Using the beforeunload hook is the best option, but note that it doesn't work consistently.

```javascript
window.addEventListener("beforeunload", function(event) {
  if (mAgent != null) {
    let states = mAgent.getAgentStates();
    // "states" is an array of changeable states. You can filter the desired state to change by name.
    let offlineState = states.filter(state => state.name === "Offline")[0];

    // Change agent state
    mAgent.setState(offlineState, {
      success: function() {
        console.log("SetState succeeded");
      },
      failure: function() {
        console.log("SetState failed");
      }
    });
  }
});
```

Step 3: Design for errors

If an API call fails to execute the first time and a contact takes the error branch of your flow, there's a chance that an agent's state won't change as expected. Be sure to include logic to account for this possibility. For example, you could delay the page unload while the API call is tried again. Or, you could pop a "Call failed" warning message in a modal dialog before the page unload.
Set up agents to assign tasks to themselves

For an agent to be able receive a task, they need a quick connect created for them. With this quick connect, agents will be able to assign tasks to themselves, and other agents will be able to assign tasks to them.

**Step 1: Create a quick connect for the agent**

1. On the navigation menu, choose Routing, Quick connects, Add a new.
2. Enter a name for the quick connect, such as the name of the agent. For example, if you want Jane Doe to be able to assign tasks to herself, enter Jane Doe.
3. Under Type, use the dropdown list to choose Agent.
4. Under Destination, use the dropdown list to choose the user name for the agent.
5. Under Flow, choose Default agent transfer, or the appropriate flow for your contact center.
6. Under Description, enter a description, such as Jane Doe's quick connect.
7. Choose Save.

The following image shows a quick connect for Jane Doe on the Quick connects page.

![Quick Connect Image](image-url)

**Step 2: Create a queue for the agent and associate the quick connect**

1. After you create the quick connect, go to Routing, Queues and add a queue for the agent.
2. On the Add new queue page, in the Quick connects box, search for the quick connect you created for the agent.
3. Select the quick connect and then choose Save.

**Step 3: Add the queue to the agent's routing profile**

1. Go to Users, Routing profiles and choose the agent's routing profile.
2. Add the agent's queue to the routing profile, and choose Task for the channel.

   If the agent can receive transfers through other channels, select them as well.

3. Choose Save.

**Set up tasks**

1. **Update your agent's routing profile** so they can manage and create tasks.

   When you add tasks to their routing profile, you can specify that up to 10 tasks be assigned to them at a time. The following image shows the Tasks option on the Routing profile page.

   ![Tasks option on Routing profile page]

2. **Create quick connects** so that agents can create/assign tasks to themselves, or other agents or shared queues.

3. Update your flows to route tasks.
4. Optionally, create task templates to make it easy for agents to create tasks. All the fields they need to create a task are defined for them.

5. Optionally, integrate with external applications and set up rules to automatically create tasks based on pre-defined conditions.

6. By default all agents can create tasks. If you want to block permissions for some agents, assign the Contact Control Panel, Restrict task creation permission in their security profile.

Create task templates

Task templates make it easy for agents to capture the right information to create and complete a task. All the fields they need to create a given type of task are provided for them.

Important things to know before you create your first template

- When you publish your first template, your agents will be prompted to select a template when they create a new task. Agents must select one of the templates you have published.

- If you want to return to the standard task experience and not require agents to select a template, on the Task templates page, use the Disable/Enable toggle to disable all templates you published.

- Verify your Amazon Connect account has permissions to create task templates.

- Review the list of quotas for task templates, such as the Task templates per instance and Task template customized fields per instance. See Amazon Connect service quotas.

How to create a task template

Step 1: Name the template

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create task templates.

2. In the left navigation menu, choose Channels, Task templates.


4. On the Create new template page, in the Template name box, enter the name that will be displayed your agents.

5. In the Description box, describe the purpose of the template. This information is not displayed to agents; it's for your own use.
Step 2: Add fields, task assignment, and schedule

1. In the **Fields** section, choose the **Add field** dropdown, and then select the type of field you want to add to your template.

2. Use the up and down arrows as needed to change the order the field appears on the template.

3. In the **Validation and permissions** section, choose whether the field is required to be populated by the agent when they create a task, or add a default value to pre-populate the field when the agent opens the template.

   The following image shows what this section looks like for a field that is type **Email**.
4. In the **Task assignment** section, choose **Yes** to allow agents to view and edit a task assignment when they create the task. Or, assign a default value, as shown in the following image. Choose a published flow that runs after the agent chooses **Create** to create the task. Agents don’t see the name of the flow on the CCP.

**Note**

It is not possible to use attributes in the task templates page.

5. In the **Task schedule** section, choose whether you want agents to be able to schedule a future start date and time for tasks.

**Step 3: Publish**

After you configure your template, choose **Publish** to create it and make it visible to your agents.

**Important**

If this is your first template, when you choose **Publish**, agents are automatically required to select a task template when they create a task.

If you want to maintain the standard task experience without selectable templates, disable all templates.
What your agents experience

After you publish a template, agents are required to select a template to create a task.

For example, the following image shows two templates have published: Customer Email Template and Billing Dispute.

In the Contact Control Panel, when agents choose Create task they must choose one of the templates: Billing Dispute or Customer Email Template.

Let's assume the agent chooses Customer Email Template. The following image shows the fields the agent must complete in order to create a task. Notice that there is no option for the agent to assign the task; this template has Task assignment set to a default value.
"No data" message in the Assign to dropdown

Let's say that in the **Task assignment** section, you choose to allow agents to assign the task to another agent. To set up for this scenario, you must create a quick connect for the destination agent so it appears in the dropdown list of choices, as shown in the following image. For instructions about creating a quick connect for an agent, see [Test tasks](#).

If no quick connects exist, then the message **No data** appears when you choose the **Assign to** dropdown menu, as shown in the following image.
Security profile permissions for task templates

Assign the **Routing, Task templates** permissions to enable a user to create task templates.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

By default, the **Admin** security profile already has permissions to perform all task activities.

### Block agents from creating tasks

To block agents from being able to create tasks, assign the **Contact Control Panel (CCP), Restrict task creation** permission. By default this permissions is unchecked, which means all agents can create tasks.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

By default, the **Admin** security profile already has permissions to perform all tasks activities.

### Set up applications for task creation

You can set up applications for task creation in just a few steps, no coding required. Amazon Connect uses Amazon EventBridge to pull data from your external application.
Tip

If your organization is using custom IAM policies to manage access to the Amazon Connect console, make sure users have the appropriate permissions to set up applications for task creation. For a list of required permissions, see Tasks page. If your instance was created before October 2018, for information about how to configure your service-linked roles (SLR), see For instances created before October 2018.

Contents

• Set up application integration for Salesforce
• Set up application integration for Zendesk
• Monitor task creation
• Disassociate an Amazon Connect connection

Set up application integration for Salesforce

If you integrate with Salesforce for event creation, Amazon Connect also uses Amazon AppFlow to put the data into EventBridge. This is because of how Salesforce sends events through the Amazon AppFlow APIs. To learn more about how Amazon Connect uses EventBridge and Amazon AppFlow resources to power Salesforce integrations, see this blog post: Building Salesforce integrations with Amazon EventBridge and Amazon AppFlow.

Note

If you use custom AWS Identity and Access Management (IAM) policies, for a list of the required IAM permissions to set up Amazon Connect Tasks, see Tasks page.

To integrate Salesforce for task creation

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. Choose **Tasks**, and then choose **Add an application**.

4. On the **Select application** page, choose **Salesforce**.

5. Review the application requirements that are listed on the **Select application** page.

The following image shows the requirements for Salesforce.
1. To verify that Salesforce is compatible with Amazon AppFlow, log in to Salesforce, for example, https://[instance_name].my.salesforce.com.

**Important**

Verify that you have enabled **Change Data Capture** in Salesforce. The following image shows an example **Change Data Capture** page in Salesforce where you select the Case entities:

![Change Data Capture page](image)

6. After you verify Salesforce requirements, on the **Select application** page, choose **Next**.
7. On the **Establish connection** page, choose one of the following:

- **Use an existing connection.** This allows you to reuse existing EventBridge resources that are linked to Amazon AppFlow flows that you may have created in your AWS account.

- **Create a new connection:** Enter the information required by the external application.

  1. Enter your application instance URL. This URL is used for deep-linking into the tasks created in your external application.

  2. Provide a friendly name for your connection, for example, **Salesforce - Test instance**. Later, when you **add rules**, you'll refer to this friendly name.

  3. Specify whether this is a production or sandbox environment.
8. Choose **Log in to Salesforce**.

9. In Salesforce, choose to allow access to Amazon Connect Embedded Login App [Region].
10. After Amazon Connect has successfully connected with the Salesforce, go to Salesforce and verify that the refresh token policy for Amazon Connect Embedded Login App is set to Refresh token is valid until revoked. This grants Amazon AppFlow access to pull data from your Salesforce account without re-authenticating.

11. On the Establish connection page, select the box shown in the following image, and choose Next.
12. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Complete integration**.

13. On the **Tasks** page, the new connection is listed.
You're done! Next, add rules that tell Amazon Connect when to create a task and how to route it. For instructions, see Create rules that generate tasks for third-party integrations.

What to do when is a connection isn't successfully established

A connection might fail to be established for Salesforce if you didn’t follow the instructions next to the check boxes to verify that it's compatible with Amazon AppFlow.

A common error is not setting up the Case entity in the Change Data Capture settings to capture these events. To fix:

1. Log in to Salesforce, go to the Change Data Capture, and select the Case entity.
2. Open the Amazon AppFlow console at https://console.aws.amazon.com/appflow to select the flow that was just created, and then choose **Activate flow**.

Alternatively, you might need to delete the Amazon AppFlow Salesforce connection and flow, and start again.

### Set up application integration for Zendesk

**Step 1: Enable the events connector for Amazon EventBridge**

If you don’t already have the EventBridge connector for Zendesk enabled, you need to set it up first. Otherwise, go to **Step 2: Integrate Zendesk with Amazon Connect for task creation**.

1. Copy your AWS account number:
a. In the Amazon EventBridge console, go to **Partner event sources**.

b. Search for or scroll to **Zendesk**, and choose **Set up**.

c. Choose **Copy** to copy your AWS account information.

2. Go to Setting up the events connector for Amazon EventBridge in the Zendesk Help and follow the instructions.

**Step 2: Integrate Zendesk with Amazon Connect for task creation**

*Note*

If you use custom AWS Identity and Access Management (IAM) policies, for a list of the required IAM permissions to set up Amazon Connect Tasks, see **Tasks page**.

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).

2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. Choose **Tasks**, and then choose **Add an application**.
4. On the **Select application** page, choose **Zendesk**.

5. After you choose to integrate with Zendesk, the application requirements are listed on the page.

   The following image shows the requirements for Zendesk. In this procedure, we walk you through the steps to select the "Support ticket" event type in Zendesk. Acknowledge the steps and choose **Next**.

6. On the **Establish connection** page, choose one of the following:
   - **Use an existing connection.** This allows you to reuse existing EventBridge resources you may have created in your AWS account.
   - **Create a new connection:** Enter the information required by the external application.
1. Enter your application instance URL. This URL is used for deep-linking into the tasks created in your external application.

2. Provide a friendly name for your connection, for example, **Zendesk - Test instance**. Later, when you add rules, you'll refer to this friendly name.
7. Choose **Copy** to copy your AWS account ID, and then choose **Login to Zendesk**. This takes you away from the **Establish connection** page for now, but you return to it shortly.

8. After you're logged in to Zendesk, choose **Connect** to connect the Events Connector for Amazon EventBridge.

9. In Zendesk, on the **Amazon Web Services** page, paste in your Amazon Web Service account ID, choose your Region, choose **Support ticket**, acknowledge the terms of use, and the choose **Connect**. Zendesk creates a resource in Amazon EventBridge.
10. Return to the **Establish connection** page in Amazon Connect choose **Next**.

11. On the **Establish connection** page, you'll see the message that Amazon Connect has successfully connected with Zendesk. Choose **Next**.
12. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Complete integration**.

This creates a connection that associates the EventBridge resource for Zendesk to Amazon Connect.

13. On the **Tasks** page, the new Zendesk connection is listed, as shown in the following image.
You're done! Next, add rules that tell Amazon Connect when to create a task and how to route it. For instructions, see [Create rules that generate tasks for third-party integrations](#).

**What to do when a connection isn't successfully established**

A connection might fail to create a task if you do not correctly select the **Support ticket** event type when setting up the connection in Zendesk, after being prompted to do so in the flow. To fix this, log in to Zendesk, and update that setting, as shown in the following image.
There is also another case where you may not have selected the correct AWS Region that the Amazon Connect instance is in, when setting up EventBridge. To fix:

2. Disconnect your EventBridge connection.
3. In the Amazon Connect console, restart the flow.

**Monitor task creation**

After your connection is established, if it stops working, in Amazon Connect disassociate the connection, and then re-establish it. If that doesn't solve the issue, do the following:

**Zendesk**

2. Check the status of the event source connection to see if it is active.
Salesforce

2. Monitor the flow that was created for the account that was set up.

The following image shows what a flow looks like in the Amazon AppFlow console for Salesforce. It contains information about the status of the connection, and when it was last run.

For both Zendesk and Salesforce, you can go to the EventBridge console at https://console.aws.amazon.com/events/ to see your connection state and see if it is active, pending, or deleted.

The following image shows an example EventBridge console.
Disassociate an Amazon Connect connection

At any time you can disassociate a connection, and stop the automatic generation of tasks based on events from the external application.

To stop the automatic generation of tasks

1. Choose the application, and then choose **Remove connection**.

2. Type **Remove**, and then choose **Remove**.
If you need to debug, you are still able to go to Amazon AppFlow (Salesforce) or EventBridge.

To remove the connection altogether from Zendesk

1. Log in to Zendesk, and navigate to https://[subdomain].zendesk.com/admin/platform/integrations.
2. Disconnect the EventBridge connection.

To remove the connection altogether from Salesforce

- Open the Amazon AppFlow console at https://console.aws.amazon.com/appflow, and delete the Salesforce connection and flow that were created in Amazon Connect.

  Flows are created with the name pattern of amazon-connect-salesforce-to-eventbridge-[subdomain].

  Connections are created with the name pattern of amazon-connect-salesforce-[subdomain]

To re-enable the automatic generation of tasks, repeat the setup steps.

Create Amazon Connect rules

A rule is an action that Amazon Connect automatically performs, based on conditions you specify. Contact center managers, supervisors and QA analysts can quickly create rules from the Amazon Connect console. No coding is required.
More information

- To create and manage rules programmatically, see Rules actions and the Amazon Connect Rules Function language in the Amazon Connect API Reference Guide.
- Alert supervisors in real-time based on keywords and phrases mentioned during a call
- Automatically categorize contacts based on keywords and phrases used during a conversation
- Create a task when a contact is categorized in real-time or post-call/chat
- Create a Contact Lens rule that generates an EventBridge event
- Create Contact Lens rules that send email notifications
- Create supervisor alerts on agent performance
- Create alerts on real-time metrics
- Create rules that generate tasks for third-party integrations

Create rules that generate tasks for third-party integrations

After you set up an external application to generate tasks automatically, you need to build rules that tell Amazon Connect when to create tasks, and how to route them.

1. Log in to Amazon Connect with a user account that is assigned the CallCenterManager security profile, or that is enabled for Rules permissions.
2. In Amazon Connect, on the navigation menu, choose Rules.
3. On the Rules page, use the Create a rule dropdown list to choose External application.
4. At the Trigger and conditions page, assign a name to the rule. Spaces are not allowed in the name of a rule.

5. Choose the event that will generate a task, and the instance of the external application where the event must occur. For example, the following image shows the trigger is when a new ticket
is created in Zendesk. The condition that must be met is when the type equals a question. Then a task is generated.

1. Select the instance for the external application.
2. Choose the conditions that must be met to generate the task.

6. Choose Next.

7. On the Action page, specify the task to be generated when the rule is met, as shown in the following image
1. The description of the task appears to the agent in their Contact Control Panel (CCP).
2. The task reference name appears to the agent as a link to the specified URL.
8. Choose Save.

Test the rule
1. Go the external application and create the event that initiates the action. For example, in Zendesk, create a ticket that's type Question.
2. Go to Analytics and optimization, Contact search.
3. Under Channel, choose Task, and then choose Search.
4. Verify the task was created.

Set up in-app, web, and video calling capabilities

The Amazon Connect in-app, web, and video calling capabilities enable your customers to contact you without ever leaving your web or mobile application. You can use these capabilities to pass contextual information to Amazon Connect. This enables you to personalize the customer experience based on attributes such as the customer's profile or other information, like actions previously taken within the app.
Communication widget: Configure chat, voice, and video all in one place

To set up in-app, web, and video calling, you use the Communication widgets page. It supports chat, voice, and video. The following image shows the Communication options section of the page when it's configured for all of these options.

![Communication options](image-url)
How to set up in-app, web, and video calling

There are two ways to embed Amazon Connect in-app, web, and video calling onto your website or mobile application:

- **Option 1**: Choose this option to set up an out-of-the-box communications widget. You can use the no-code UI builder to customize the font and colors, and secure the widget so that it can be launched only from your website.

- **Option 2**: Choose this option to build a communications widget from scratch and integrate it with your mobile application or website. Use the Amazon Connect APIs and Amazon Chime SDK client APIs to integrate natively into your mobile application or website.

**Note**

If you have custom agent desktops, you don’t need to make any changes for Amazon Connect in-app and web calling. However, you need to integrate video calling.

**Option 1: Configure an out-of-the-box communication widget**

Use this option to create communication widgets for desktop and mobile browsers. At the end of this procedure, Amazon Connect generates a custom HTML code snippet that you copy into your website's source code.

1. Log in to Amazon Connect admin website using an Admin account or a user account that has Channels and flows, Communication widget - Create permission in its security profile.

2. In Amazon Connect, on the left navigation menu, choose Channels, Communication widgets.

3. The wizard guides you through the next three steps.

**Step 1: Select communication channels**

1. On the Communication widgets page, enter a Name and Description for the communications widget.
Note
The Name must be unique for each communications widget created in an Amazon Connect instance.

2. In the **Communications options** section, choose how your customers can engage with your widget. The following image shows options to allow web calling and video for customers.

3. In the **Web calling** section, choose whether to enable voice or video experiences for your customers. The previous image shows Web calling options with video enabled for customers to see agent video and to allow customers to turn on their video.
4. Choose **Save and continue**.

**Step 2: Customize widget**

As you choose these options, the widget preview updates automatically so that you can see what the experience will look like for your customers.

![Widget Preview](image)

**Define widget access button styles**

1. Choose the colors for the button background by entering hex values ([HTML color codes](https://www.w3schools.com/html/html_color_codes.asp)).
2. Choose **White** or **Black** for the icon color. The icon color can't be customized.

**Customize display names and styles**

1. Provide values for header message and color, and widget background color.
2. **Logo URL**: Insert a URL to your logo banner from an Amazon S3 bucket or another online source.
**Note**

The communications widget preview in the customization page will not display the logo if it's from an online source other than an Amazon S3 bucket. However, the logo will be displayed when the customized communications widget is implemented to your page.

The banner must be in .svg, .jpg or .png format. The image can be 280px (width) by 60px (height). Any image larger than those dimensions will be scaled to fit the 280x60 logo component space.

1. For instructions about how to upload a file such as your logo banner to S3, see [Uploading objects](amazonaws.com) in the *Amazon Simple Storage Service User Guide*.

2. Make sure that the image permissions are properly set so that the communications widget has permissions to access the image. For information about how to make a S3 object publicly accessible, see [Step 2: Add a bucket policy](amazonaws.com) in the *Setting permissions for website access* topic.

**Step 3: Add your domain for the widget**

This step enables you to secure the communications widget so that it can be launched only from your website.

1. Enter the website domains where you want to place the communications widget. The communications widget loads only on websites that you select in this step.

   Choose **Add domain** to add up to 50 domains.
1. **Add the required domains for the communication widget**

   Add the website domains where you want the communication widget to display. For example https://www.yourcompany.com or https://support.yourcompany.com.

   This is required to validate the origin of the communication widget requests. [Learn more](#)

   | 1:   | https://mydomain01.com       |
   | 2:   | https://mydomain02.com       |

   ![Add domain button](image)

   - **Important**
     - Double-check that your website URLs are valid and does not contain errors. Include the full URL starting with https://.
     - We recommend using https:// for your production websites and applications.

2. Under **Add security for your communications widget requests**, for the fastest setup experience choose **No - I will skip**.

   We recommend choosing **Yes** for the ability to verify the user is authenticated. For more information, see [Passing attributes for in-app, web, and video calling](#).

3. Choose **Save and continue**.

   Success! Your widget has been created. Copy the generated code and paste it on each page of your website where you want the communications widget to appear.

### Enable your agents for in-app, web, and video-calling

To enable agents to use video calling, assign the **Contact Control Panel (CCP), Video calls - Access** permissions to their security profile.

The Amazon Connect agent workspace supports Amazon Connect in-app, web, and video calling. You can use the same configuration, routing, analytics, and agent application as with telephone calls and chats. To get started, the only step is to enable your agent’s security profiles with the permissions to have video calls.
For custom agent desktops, there are no changes required for the Amazon Connect in-app and web calling. Enable your agent's security profiles with the permissions to have video calls, and follow the guide below on how to integrate video calling into your agent desktop.

**How a client device initiates an in-app or web call**

The following diagram shows the sequence of events for a client device (mobile application or browser) to initiate an in-app or web call.

1. (Optional) You can pass attributes captured in the website and validate them with JSON web token (JWT).
2. The customer clicks on the communications widget in your website or mobile app.
3. The communications widget starts the web call to Amazon Connect by passing attributes contained in the JWT.
4. The contact reaches the flow, is routed, and placed in queue.
5. The agent accepts the contact.
6. (Optional) If video is enabled for customer and the agent, they are able to start their video.

**Option 1: Configure an out-of-the-box communication widget**
More information

For additional information about requirements for in-app, web, and video calling capabilities, see the following topics:

- Agent workstation networking requirements for web calling voice/video
- Supported browsers and mobile OS for in-app, web, and video calling capabilities

Option 2: Integrate in-app, web, and video calling natively into your mobile application using the Amazon Chime SDK client APIs

To integrate Amazon Connect in-app, web, and video calling natively with your mobile application use the Amazon Connect StartWebRTCContact API to create the contact, and then use the details returned by the API call to join the call using the Amazon Chime client library for iOS or Android.

How a client device initiates an in-app or web call

The following diagram shows the sequence of events for a client device (mobile application or browser) to initiate an in-app or web call.
1. Your customer uses the client application (website or application) to start an in-app or web call.

2. The client application (website or mobile application) or web server uses the Amazon Connect `StartWebRTCContact` API to start the contact passing any attributes or context to Amazon Connect.

3. The client application joins the call using the details returned from the `StartWebRTCContact` in step 1.

4. (Optional) Client uses the `CreateParticipantConnection` API to receive a `ConnectionToken` that is used to send DTMF through the `SendMessage` API.

5. The contact reaches the flow and is routed based on the flow and placed in queue.

6. The agent accepts the contact.

7. (Optional) If video is enabled for customer and the agent, they are able to start their video.

Option 2: Integrate in-app, web, and video calling natively into your mobile application
Get started

Following are the high level steps to get started:

1. Use the `StartWebRTCContact` API to create the contact. The API returns the details needed for the Amazon Chime client SDK to join the call.

2. Instantiate the Amazon Chime SDK client `MeetingSessionConfiguration` object using the configurations returned by `StartWebRTCContact`.

3. Instantiate Amazon Chime SDK client `DefaultMeetingSession` with `MeetingSessionConfiguration`, which was created in step 2 to create a client meeting session.
   - iOS (Swift)

   ```swift
   let logger = ConsoleLogger(name: "logger")
   let meetingSession = DefaultMeetingSession(configuration: meetingSessionConfig,
                                             logger: logger)
   ```

   - Android (Kotlin)

   ```kotlin
   val logger = ConsoleLogger()
   val meetingSession = DefaultMeetingSession(
                                           configuration = meetingSessionConfig,
                                           logger = logger,
                                           context = applicationContext
   )
   ```

4. Use the `meetingSession.audioVideo.start()` method to join the WebRTC contact with audio.

5. Use the `meetingSession.audioVideo.stop()` method to hangup the WebRTC contact.

6. Optional steps
   a. To send DTMF to the call, two Amazon Connect Participant Service APIs are needed: `CreateParticipantConnection` and `SendMessage` respectively.

      ```plaintext
      Note
      contentType for the SendMessage API must be audio/dtmf.
      ```
i. Invoke **CreateParticipantConnection** to retrieve ConnectionToken. (ParticipantToken is needed for calling this API. You can find it in the **StartWebRTCContact** response.)

ii. With the ConnectionToken, call **SendMessage** for sending DTMF digits.

b. For mute and unmute, use `meetingSession.audioVideo.realtimeLocalMute()` and `meetingSession.audioVideo.realtimeLocalUnmute()`.

c. To start self video on the mobile application, use the `meetingSession.audioVideo.startLocalVideo()`.

d. To stop self video on the mobile application, use the `meetingSession.audioVideo.stopLocalVideo()`.

e. To allow receiving and loading video of the agent inside mobile application, use the `meetingSession.audioVideo.startRemoteVideo()`.

f. To disallow receiving and loading video of the agent inside mobile application, use the `meetingSession.audioVideo.stopRemoteVideo()`.

g. To select the audio input/output device, you can use the methods from the Amazon Chime SDK client for Android and iOS or the [native iOS capabilities](#) for iOS.

**Passing attributes for in-app, web, and video calling**

The steps in this topic are optional but recommended. They enable you to personalize the customer’s experience based on their actions previously taken within your app. This option provides you more control when initiating new calls, including the ability to pass contextual information as attributes.

After doing these steps, you'll need to work with your website administrator to set up your web servers to issue JSON Web Tokens (JWTs) for new calls

1. If you've already created your communications widget, on the **Communication widgets** page, choose the widget to edit it.

2. In the **Domain & Security** section, choose **Edit**.

3. Under **Add security for your communications widget requests**, choose **Yes**.
4. Choose **Save and continue**. Amazon Connect creates the widget along with the following:

- Amazon Connect provides a 44-character security key on the next page that you can use to create JWTs.
- Amazon Connect adds a callback function within the communications widget embed script that checks for a JWT when a call is initiated.

You must implement the callback function in the embedded snippet, as shown in the following example.

```javascript
amazon_connect('authenticate', function(callback) {
    window.fetch('/token').then(res => {
        res.json().then(data => {
            callback(data.data);
        });
    });
});
```

In the next step you'll get a security key for all calls initiated on your websites. Ask your website administrator to set up your web servers to issue JWTs using this security key.

5. Choose **Save and continue**.

6. Copy the custom HTML code snippet and insert it into your website's source code.

### Copy communications widget code and security keys

In this step, you confirm your selections and copy the code for the communications widget and embed it in your website. You can also copy the secret keys for creating the JWTs.
Security key

Use this 44-character security key to generate JSON web tokens from your web server. You can also update, or rotate, keys if you need to change them. When you do this, Amazon Connect provides you with a new key and maintains the previous key until you have a chance to replace it. After you have the new key deployed, you can come back to Amazon Connect and delete the previous key.

When your customers interact with the start call icon on your website, the communications widget requests your web server for a JWT. When this JWT is provided, the widget will then include it as part of the end customer’s call to Amazon Connect. Amazon Connect then uses the secret key to decrypt the token. If successful, this confirms that the JWT was issued by your web server and Amazon Connect routes the call to your contact center agents.

JSON Web Token specifics

- Algorithm: **HS256**
- Claims:
  - **sub**: `widgetId`
    
    Replace `widgetId` with your own `widgetId`. To find your `widgetId`, see the example Communications widget script.
  - **iat**: *Issued At Time.
  - **exp**: *Expiration (10 minute maximum).

* For information about the date format, see the following Internet Engineering Task Force (IETF) document: [JSON Web Token (JWT)](https://tools.ietf.org/html/rfc7519), page 5.

The following code snippet shows an example of how to generate a JWT in Python:

```python
payload = {
    'sub': 'widgetId',  # don't add single quotes, such as 'widgetId'
}```
Communications widget script

The following image shows an example of the JavaScript that you embed on the websites where you want customers to be able to call your contact center. This script displays the widget in the bottom-right corner of your website.

The following image shows an example of where to find your widgetId.

Please follow these two steps to deploy your customized communication widget.

1 Widget script

Copy this generated code and paste it on each page of your website where you want the communication widget to appear.

```html
<script type="text/javascript">
(function(w, d, x, id){
 s=d.createElement('script');
 s.src='https://dnczz2s468gpz.cloudfront.net/amazon-connect-chat-interface-client.js';
 s.async=1;
 s.id=id;
 d.getElementsByTagName('head')[0].appendChild(s);
 w[x] = w[x] || function() { (w[x].ac = w[x].ac || []).push(arguments) };
 })(window, document, 'amazon_connect', '0a37cb74-e8e2-4700-bec7-c7cd222ece9e');
 amazon_connect('styles', { iconType: 'CHAT_VOICE', openChat: { color: '#ffffff', backgroundColor: '#123456' }, closeChat: { color: '#ffffff', backgroundColor: '#123456' } });
 amazon_connect('snippetId', 'QVFJREFlak...');
 amazon_connect('supportedMessagingContentTypes', [ 'text/plain', 'text/markdown' ]);  
</script>
```
When your website loads, customers first see the **Start** icon. When they choose this icon, the communications widget opens and customers are able to call your agents.

To make changes to the communications widget at any time, choose **Edit**.

**Note**

Saved changes update the customer experience in a few minutes. Confirm your widget configuration before saving it.
To make changes to widget icons on the website, you will receive a new code snippet to update your website directly.

**Integrate video calling into your custom agent desktop**

For custom agent desktops, you need to make changes to support video calling. Following are high level steps.

1. Use Amazon Connect Streams JS to check if the incoming contact is a WebRTC contact. Use contact subtype "connect:WebRTC", as shown in the following code example:

   ```
   contact.getContactSubtype() === "connect:WebRTC"
   ```

2. You can retrieve the customer display name by using the name field in contact.getName().

Following are additional steps for video handling if your customers have enabled it on their end:

1. To check whether a contact has video capability:

   ```
   // Return true if any connection has video send capability
   contact.hasVideoRTCCapabilities()

   // Return true if the agent connection has video send capability
   contact.canAgentSendVideo()

   // Return true if other non-agent connection has video send capability
   contact.canAgentReceiveVideo()
   ```

2. To check on whether the agent has video permission to handle video call:

   ```
   agent.getPermissions().includes('videoContact');
   ```

3. To accept a video call, the contact must have video capability and the agent must have video permission.
function shouldRenderVideoUI() {
    return contact.getContactSubtype() === "connect:WebRTC" &&
    contact.hasVideoRTCCapabilities() &&
    agent.getPermission().includes('videoContact');
}

4. In order to join a video session, call `getVideoConnectionInfo`:

```javascript
if (shouldRenderVideoUI()) {
    const response = await contact.getAgentConnection().getVideoConnectionInfo();
}
```

5. To build a video UI and join a video meeting session, see:
   - [Amazon Chime SDK for JavaScript](https://github.com/aws/amazon-chime-sdk-js) on GitHub
   - [Amazon Chime SDK React Components Library](https://github.com/aws/amazon-chime-sdk-component-library-react) on GitHub

6. For simplicity, the following code snippets use examples from the Amazon Chime SDK React Components Library.

```javascript
import { MeetingSessionConfiguration } from "amazon-chime-sdk-js";
import {
    useMeetingStatus,
    useMeetingManager,
    MeetingStatus,
    DeviceLabels,
    useLocalAudioOutput
} from 'amazon-chime-sdk-component-library-react';

const App = () => (
    <MeetingProvider>
        <MyVideoManager />
    </MeetingProvider>
);

const MyVideoManager = () => {
    const meetingManager = useMeetingManager();
    if (shouldRenderVideoUI()) {
        const response = await contact.getAgentConnection().getVideoConnectionInfo();
        const configuration = new MeetingSessionConfiguration(
            response.meeting, response.attendee)
```
await meetingManager.join(configuration, { deviceLabels: DeviceLabels.Video });
    await meetingManager.start();
}

function endContact() {
    meetingManager.leave();
}

7. To render the video grid, use the VideoTileGrid from the Amazon Chime SDK React Components Library or customize the UI behavior using RemoteVideoTileProvider.

8. To render a video preview, you can use VideoPreview and CameraSelection components. To choose or change a camera video, you can use meetingManager.selectVideoInputDevice or meetingManager.startVideoInput if the meeting is in progress.

const meetingManager = useMeetingManager();
const { isVideoEnabled } = useLocalVideo();
if (isVideoEnabled) {
    await meetingManager.startVideoInputDevice(current);
} else {
    meetingManager.selectVideoInputDevice(current);
}

9. To implement background blur, see useBackgroundBlue.

10. For sample code on how to build a custom video experience, see this Amazon Chime SDK sample: Amazon Chime React Meeting demo.

Set up your customer's chat experience

You can provide a chat experience to your customers by using one of the following methods:

- Add a chat user interface to your website.
- Download and customize our open source example.
- Customize your solution using Amazon Connect APIs. We recommend starting with the Amazon Connect ChatJS open source library when customizing your own chat experiences. For more information, see the Amazon Connect ChatJS repo on Github.
More resources to customize the chat experience

- Interactive messages provide customers with a prompt and pre-configured display options that they can select from. These messages are powered by Amazon Lex and configured through Amazon Lex using a Lambda. For instructions about how to add interactive messages through Amazon Lex, see this blog: Set up interactive messages for your Amazon Connect chatbot.

Amazon Connect supports the following templates: a list picker and a time picker. For more information, see Add interactive messages to chat.

- Enable Apple Messages for Business
- Amazon Connect Service API Documentation, especially the StartChatContact API.
- Amazon Connect Participant Service API.
- Amazon Connect Chat SDK and Sample Implementations
- Amazon Connect Streams. Use to integrate your existing apps with Amazon Connect. You can embed the Contact Control Panel (CCP) components into your app.

Add a chat user interface to your website

To support your customers through chat, you can add a communications widget to your website that is hosted by Amazon Connect. You can configure the communications widget in the Amazon Connect admin website: customize the font and colors, and secure the widget so that it can be launched only from your website. As a result, you will have a short code snippet that you add to your website.

Because Amazon Connect hosts the widget, it ensures that the latest version is always live on your website.

Tip

Use of the communications widget is subject to default service quotas, such as the number of required characters for each message. Before launching your communications widget into production, make sure that your service quotas are set for your organization's needs. For more information, see Amazon Connect service quotas.
Supported browsers

The pre-built communications widget supports the following browser versions and higher:

- Google Chrome 85.0
- Safari 13.1
- Microsoft Edge version 85
- Mozilla Firefox 81.0

The communications widget supports browser notifications for desktop devices. For more information, see Browser notifications.

Step 1: Customize your communications widget

In this step, you customize the experience of the communications widget for your customers.

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Choose Customize communications widget.

2. On the Communications widgets page, choose Add communications widget to begin customizing a new communications widget experience. To edit, delete, or duplicate an existing communications widget, choose from the options under the Actions column, as shown in the following image.

Add a chat user interface to your website
3. Enter a **Name** and **Description** for the communications widget.

**Note**

The Name must be unique for each communications widget created in an Amazon Connect instance.

4. In the **Communications options** section, choose how your customers can engage with your widget, and then choose **Save and continue**. The following image shows options to allow chat and message receipts for customers.
5. On the **Create communication widget** page, choose the widget button styles, and display names and styles.

As you choose these options, the widget preview updates automatically so that you can see what the experience will look like for your customers.
**Button styles**

1. Choose the colors for the button background by entering hex values ([HTML color codes](https://www.w3schools.com/tags/att_style_color.asp)).
2. Choose **White** or **Black** for the icon color. The icon color can't be customized.

**Widget header**

1. Provide values for header message and color, and widget background color.
2. **Logo URL:** Insert a URL to your logo banner from an Amazon S3 bucket or another online source.
Note

The communications widget preview in the customization page will not display the logo if it's from an online source other than an Amazon S3 bucket. However, the logo will be displayed when the customized communications widget is implemented to your page.

The banner must be in .svg, .jpg or .png format. The image can be 280px (width) by 60px (height). Any image larger than those dimensions will be scaled to fit the 280x60 logo component space.

1. For instructions about how to upload a file such as your logo banner to S3, see [Uploading objects](#) in the *Amazon Simple Storage Service User Guide*.

2. Make sure that the image permissions are properly set so that the communications widget has permissions to access the image. For information about how to make a S3 object publicly accessible, see [Step 2: Add a bucket policy](#) in the *Setting permissions for website access* topic.

Chat view

1. **Typeface**: Use the dropdown to choose the font for the text in the communications widget.

2. • **System Message Display Name**: Type a new display name to override the default. The default is `SYSTEM_MESSAGE`.

   • **Bot Message Display Name**: Type a new display name to override the default. The default is `BOT`.

   • **Text Input Placeholder**: Type new placeholder text override the default. The default is `Type a message`.

   • **End Chat Button Text**: Type new text to replace the default. The default is `End chat`.

3. **Agent chat bubble color**: Choose the colors for the agent's message bubbles by entering hex values ([HTML color codes](#)).

4. **Customer chat bubble color**: Choose the colors for the customer's message bubbles by entering hex values ([HTML color codes](#)).

5. Choose **Save and continue**.
Step 2: Specify the website domains where you expect to display the communications widget

1. Enter the website domains where you want to place the communications widget. Chat loads only on websites that you select in this step.

Choose Add domain to add up to 50 domains.

1. Add the required domains for the Communication widget

   Add the website domains where you want the communication widget to display. For example https://www.yourcompany.com or https://support.yourcompany.com. This is required to validate the origin of the communication widget requests.

   1: https://mydomain01.com
   2: https://mydomain02.com

   [Add domain button]

   Learn more

   Important
   - Double-check that your website URLs are valid and does not contain errors. Include the full URL starting with https://.
   - We recommend using https:// for your production websites and applications.

2. Under Add security for your communications widget, we recommend choosing Yes, and working with your website administrator to set up your web servers to issue JSON Web Tokens (JWTs) for new chat requests. This provides you more control when initiating new chats, including the ability to verify that chat requests sent to Amazon Connect are from authenticated users.
Add security for new communication widget requests

We recommend using JSON web tokens to secure new communication widget requests. This provides you more control when initiating requests from the new communication widget, including the ability to verify that requests sent to Amazon Connect are from authenticated users. This implementation is typically completed by a website administrator. Learn how to set this up.

Would you prefer to do this?

- Yes
- No - I will skip this step

Choosing Yes results in the following:

- Amazon Connect provides a 44-character security key on the next page that you can use to create JWTs.
- Amazon Connect adds a callback function within the communications widget embed script that checks for a JWT when a chat is initiated.

You must implement the callback function in the embedded snippet, as shown in the following example.

```
amazon_connect('authenticate', function(callback) {
  window.fetch('/token').then(res => {
    res.json().then(data => {
      callback(data.data);
    });
  });
});
```

If you choose this option, in the next step you'll get a security key for all chat requests initiated on your websites. Ask your website administrator to set up your web servers to issue JWTs using this security key.

3. Choose Save.
Step 3: Confirm and copy communications widget code and security keys

In this step, you confirm your selections and copy the code for the communications widget and embed it in your website. If you chose to use JWTs in Step 2, you can also copy the secret keys for creating them.

Security key

Use this 44-character security key to generate JSON web tokens from your web server. You can also update, or rotate, keys if you need to change them. When you do this, Amazon Connect provides you with a new key and maintains the previous key until you have a chance to replace it. After you have the new key deployed, you can come back to Amazon Connect and delete the previous key.

When your customers interact with the Start chat icon on your website, the communications widget requests your web server for a JWT. When this JWT is provided, the widget will then include it as part of the end customer’s chat request to Amazon Connect. Amazon Connect then uses the secret key to decrypt the token. If successful, this confirms that the JWT was issued by your web server and Amazon Connect routes the chat request to your contact center agents.

JSON Web Token specifics

- **Algorithm:** HS256
- **Claims:**
  - **sub:** `widgetId`  
    Replace `widgetId` with your own `widgetId`. To find your `widgetId`, see the example Communications widget script.
  - **iat:** *Issued At Time.
  - **exp:** *Expiration (10 minute maximum).
* For information about the date format, see the following Internet Engineering Task Force (IETF) document: JSON Web Token (JWT), page 5.

The following code snippet shows an example of how to generate a JWT in Python:

```python
payload = {
    'sub': widgetId, // don't add single quotes, such as 'widgetId'
    'iat': datetime.utcnow(),
    'exp': datetime.utcnow() + timedelta(seconds=JWT_EXP_DELTA_SECONDS)
}

header = {
    'typ': "JWT",
    'alg': 'HS256'
}

encoded_token = jwt.encode(payload, CONNECT_SECRET, algorithm=JWT_ALGORITHM, headers=header) // CONNECT_SECRET is the security key provided by Amazon Connect
```

**Communications widget script**

The following image shows an example of the JavaScript that you embed on the websites where you want customers to chat with agents. This script displays the widget in the bottom-right corner of your website.
1. An example of where to find your widgetId.

When your website loads, customers first see the **Start** icon. When they choose this icon, the communications widget opens and customers are able to send a message to your agents.

To make changes to the communications widget at any time, choose **Edit**.

**Note**

 Saved changes update the customer experience in a few minutes. Confirm your widget configuration before saving it.
To make changes to widget icons on the website, you will receive a new code snippet to update your website directly.

**Getting error messages?**

If you encounter error messages, see [Investigate common issues with adding a chat user interface to your website](#).

**More customizations for your communications widget**

See the following topics for more you can do to customize the chat experience:
- **Customize widget launch behavior and button icon**
- **Pass the customer display name when a chat initializes**
- **Pass contact attributes when a chat initializes**
- **Enable message *Delivered* and *Read* receipts in your chat user interface**

**Customize widget launch behavior and button icon**

To further customize how your website renders and launches the hosted widget icon, you can configure the launch behavior and hide the default icon. For example, you can programmatically launch the widget from a **Chat with us** button element that is rendered on your website.

**How to configure custom launch behavior for the widget**

To pass custom launch behavior, use the following example code block and embed it in your widget. All of the fields shown in the following example are optional and any combination can be used.

```javascript
amazon_connect('customLaunchBehavior', {
  skipIconButtonAndAutoLaunch: true,
  alwaysHideWidgetButton: true,
  programaticLaunch: (function(launchCallback) {
    var launchWidgetBtn = document.getElementById('launch-widget-btn');
    if (launchWidgetBtn) {
      launchWidgetBtn.addEventListener('click', launchCallback);
      window.onunload = function() {
        launchWidgetBtn.removeEventListener('click', launchCallback);
        return;
      }
    }
  })
});
```

**Supported options and constraints**

The following table lists the supported custom launch behavior options. Fields are optional and any combination can be used.
<table>
<thead>
<tr>
<th>Option name</th>
<th>Type</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>skipIconButtonAndAutoLaunch</td>
<td>Boolean</td>
<td>A flag to enable/disable the automatic launch of the widget without the user clicking on the page load.</td>
<td>undefined</td>
</tr>
<tr>
<td>alwaysHideWidgetButton</td>
<td>Boolean</td>
<td>A flag to enable/disable the widget icon button from rendering (unless there is an ongoing chat session).</td>
<td>undefined</td>
</tr>
<tr>
<td>programmaticLaunch</td>
<td>Function</td>
<td></td>
<td>undefined</td>
</tr>
</tbody>
</table>

Configure widget launch for custom use cases

Custom widget launch button

The following example shows changes you would need to make in the widget to configure programmatic launch to open only when the user chooses a custom button element rendered anywhere on your website. For example, they may choose a button named **Contact Us** or **Chat With Us**. Optionally, you can hide the default Amazon Connect widget icon until the widget has been opened.

```html
<button id="launch-widget-btn">Chat With Us</button>
```

```javascript
(function(w, d, x, id){
    s=d.createElement("script");
    s.src="/amazon-connect-chat-interface-client.js"
    s.async=1;
    s.id=id;
    d.getElementsByTagName("head")[0].appendChild(s);
})(window, document, 'amazon-connect-chat', 'amazon-connect-chat');
```
Hyperlink support

The following example shows changes you would need to make in the widget configure auto-launch, which opens the widget without waiting for the user to click. You can deploy to a page that hosted by your website to create a shareable hyperlink.

https://example.com/contact-us?autoLaunchMyWidget=true
Load widget assets when button is clicked

The following example shows changes you would need to make in the widget to make your website page load faster by fetching the widget's static assets when a user clicks the Chat With Us button. Typically, only small percentage of customers visiting a Contact Us page open the Amazon Connect widget. The widget could be adding latency on page load by fetching files from CDN, even though customers never open the widget.

An alternative solution is to run the snippet code asynchronously (or never) on button click.

```html
<button id="launch-widget-btn">Chat With Us</button>
```

```javascript
var buttonElem = document.getElementById('launch-widget-btn');

buttonElem.addEventListener('click', function() {
    (function(w, d, x, id){
        s=d.createElement("script");
        s.src='./amazon-connect-chat-interface-client.js'
        s.async=1;
        s.id=id;
        d.getElementsByTagName("head")[0].appendChild(s);
        w[x] =  w[x] || function() { (w[x].ac = w[x].ac || []).push(arguments) };
    })(window, document, 'amazon_connect', 'asfd-asdf-asfd-asdf-asdf');
    amazon_connect('styles', { openChat: { color: '#000', backgroundColor: '#3498fe'},
    closeChat: { color: '#fff', backgroundColor: '#123456'} });
    amazon_connect('snippetId', "QVFJREFsdafsdfsadfsdafsdfsdasdfsdfsz0=")
    amazon_connect('customLaunchBehavior', {
        skipIconButtonAndAutoLaunch: true
    });
});
```

Launch a new chat in a browser window

The following example shows changes you would need to make in the widget to launch a new browser window and auto-launch chat in a full screen.

```html
<button id="openChatWindowButton">Launch a Chat</button>
```
Pass the customer display name when a chat initializes

To deliver a more personalized experience for both your customers and agents, you can customize the Amazon Connect communications widget to pass the customer display name during contact initialization. The name is visible to both the customer and agent throughout the chat interaction. This display name is recorded in the chat transcript.

The following images show the customer's display name in their chat experience, and their name in the agent's CCP.
1. How the customer display name may appear to the customer using the chat user interface.
2. How the customer display name may appear to the agent using the CCP.

**How to pass a customer display name in the communications widget**

To pass a customer display name, implement your callback function in the snippet. Amazon Connect retrieves the display name automatically.

1. Complete the steps in [Add a chat user interface to your website](#), if you haven't already.
2. Augment your existing widget snippet to add a `customerDisplayName` callback. It might look something like the following example:

   ```javascript
   amazon_connect('customerDisplayName', function(callback) {
       const displayName = 'Jane Doe';
       callback(displayName);
   });
   ```

   The important thing is that the name is passed to `callback(name)`.

**Things you need to know**

- Only one `customerDisplayName` function can exist at a time.
- The customer display name must follow the limitations set by the [StartChatConnect](#) API. That is, the name must be a string between 1 and 256 characters.
An empty string, null, or undefined is invalid input for the display name. To protect against accidentally passing of these inputs, the widget logs an error, Invalid customerDisplayName provided, in the browser console, and then starts the chat with the default display name, Customer.

Because the snippet is in the front end of your website, do not pass sensitive data as the display name. Be sure to follow the appropriate security practices to keep your data safe and protect against attacks and bad actors.

Pass contact attributes when a chat initializes

You can use contact attributes to capture information about the contact who is using the communications widget. Then, you can display that information to the agent through the Contact Control Panel (CCP), or use it elsewhere in the flow.

For example, you can customize your flow to say the name of the customer in your welcome message. Or, you can use attributes specific to your business, such as account/member IDs, customer identifiers like names and emails, or other metadata associated with a contact.

How to pass contact attributes into the communications widget

1. Enable security in the communications widget as described in Add a chat user interface to your website, if you haven't already:
   a. In Step 2, under Add security for your chat widget, choose Yes.
   b. In Step 3, use the security key to generate JSON web tokens.
2. Add the contact attributes to the payload of your JWT as an attributes claim.

   Following is an example of how you might generate a JWT with contact attributes in Python:

   ```python
   import jwt

   CONNECT_SECRET = "your-securely-stored-jwt-secret"

   payload = {
       'sub': 'widget-id',
       'iat': datetime.datetime.utcnow(),
       'exp': datetime.datetime.utcnow() + datetime.timedelta(seconds=500),
       'attributes': {"name": "Jane", "memberID": "123456789", "email": "Jane@example.com", "isPremiumUser": "true", "age": "45"}
   }
   ```
In the payload, you must create a string key attributes (as-is, all lowercase), with an object as its value. That object must have string-to-string key-value pairs. If anything other than a string is passed in any one of the attributes, the chat will fail to start.

The contact attributes must follow the limitations set by the StartChatConnect API:

- Keys must have a minimum length of 1
- Values can have a minimum length of 0

**Things you need to know**

- The communications widget has a 6144 bytes limit for the entire encoded token. Because JavaScript uses UTF-16 encoding, 2 bytes are used per character, so the maximum size of the encoded_token should be around 3000 characters.
- The encoded_token should be passed in to callback(data). The authenticate snippet does not need any additional changes. For example:

```javascript
amazon_connect('authenticate', function(callback) {
    window.fetch('/token').then(res => {
        res.json().then(data => {
            callback(data.data);
        });
    });
});
```

- Using a JWT to pass contact attributes ensures the integrity of the data. If you safeguard the shared secret and follow appropriate security practices, you can help ensure that the data cannot be manipulated by a bad actor.
- Contact attributes are only encoded in the JWT, not encrypted, so it’s possible to decode and read the attributes. Sensitive data should not be passed in the token.
If you want to test the chat experience with the simulated chat experience and include contact attributes, be sure to enclose both the key and value in quotes, as shown in the following image.

![Test Settings](image)

**Download and customize our open source example**

You can further customize the chat experience customers use to interact with agents. Use the Amazon Connect open source library on GitHub. It's a platform to help you get started quickly. Here's how it works:

- The GitHub repository links to a CloudFormation template, which starts the Amazon API Gateway endpoint that initiates a Lambda function. You can use this template as an example.
- After you create the AWS CloudFormation stack, you can call this API from your app, import the pre-built communications widget, pass the response to the widget, and start chatting.

For more information about customizing the chat experience, see:

- Amazon Connect Service API Documentation, especially the `StartChatConnect` API.
- Amazon Connect Participant Service API.
- Amazon Connect Streams. Use to integrate your existing apps with Amazon Connect. You can embed the Contact Control Panel (CCP) components into your app.
- Amazon Connect Chat SDK and Sample Implementations

**Start chats using your own applications**

You can use Amazon Connect APIs to start chats in your own applications.

The `StartChatConnect` API is used to start the chat.
When you explore the chat experience for the first time, you'll notice that chats aren't counted in the **Contacts Incoming** metric in your historical metrics report. This is because the initiation method for the chat in the contact record is **API**.

The following image of a contact record shows the *Initiation Method* set to *API*.

![Contact Trace Record](image)

After a chat is transferred to an agent, the **Contacts Incoming** metric is incremented. The contact record for the transfer no longer increments the API, but it does increment **Contacts Incoming**.

**Browser notifications**

The communications widget supports browser notifications for your customers through their desktop devices. Specifically, your customers will receive a notification through their web browser when they receive a new message, but are not active on the webpage that contains the chat window. When your customers click or tap this notification, they are automatically redirected to the webpage containing the chat window. Your customers can enable or disable notifications at the start of each chat conversation.

The following image shows an example of the notification banner that customers receive when they are not on the webpage that contains the chat window. The banner tells your customers that they have a new message, and it displays the name of the website.
Customers also receive a notification icon—a red dot—on the communications widget when it is minimized. The following image shows an image of the notification icon that customers receive when their chat window is minimized.

![Notification Icon](image)

Both of these features are automatically included in the communications widget. You don't need to perform any steps to make them available to your customers.

Your customers receive a pop-up to allow/deny notification when they initiate a chat and have not yet allowed notifications from your website or domain. After they grant notification permissions, they start receiving browser notifications for any message or attachment sent by the agent when they are not on the webpage with the chat window. This behavior applies even if you've already implemented the communications widget.

**How to test**

1. After you allow notifications as a test customer and the agent is connected to the chat, minimize your chat window and then open a new browser instance so you aren't on the webpage that contains the chat window.

2. Send a message from the agent window.

3. As the test customer, you'll see the notification banner.

4. Choose or tap the notification banner. You'll automatically go to the webpage that contains the chat window.

5. Because you minimized your chat window earlier, you will also see a notification icon—a red dot—on the communications widget.

If you can't see the browser notification, check the following:

- You're using a supported browser.
- The notification permission is allowed/enabled on your browser for the webpage with chat window.
• The agent (or you from your agent chat session) has sent a new message/attachment while you're on a webpage that is different from the one that contains the chat window. For the notification icon—a red dot—on the widget to be visible, minimize your chat window.

• Notifications from the browser are not snoozed (temporarily dismissed).

**Pass custom styles to override the defaults in the communications widget**

To further customize your chat user interface, you can override the default styles by passing your own values. For example, you can set the widget width to 400 pixels and the height to 700 pixels (in contrast to the default size of 300 pixels by 540 pixels). You can also use your preferred font colors and sizes.

**How to pass custom styles for the communications widget**

To pass custom styles, use the following example code block and embed it in your widget. Amazon Connect retrieves the custom styles automatically. All of the fields shown in the following example are optional.

```javascript
amazon_connect('customStyles', {
    global: {
        frameWidth: '400px',
        frameHeight: '700px',
        textColor: '#fe3251',
        fontSize: '20px',
        footerHeight: '120px',
    },
    header: {
        headerTextColor: '#541218',
    },
    transcript: {
        messageFontSize: '13px',
        messageTextColor: '#fe3'
    },
    footer: {
        buttonFontSize: '20px',
        buttonTextColor: '#ef18d3',
    }
})
```
Supported styles and constraints

The following table lists the supported custom style names and recommended value constraints. Some styles exist at both the global and component levels. For example, the fontSize style exists globally and in the transcript component. Component level styles have higher priority and will be honored on the chat widget.

<table>
<thead>
<tr>
<th>Custom style name</th>
<th>Description</th>
<th>Recommended constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>global.frameWidth</td>
<td>Width of the entire widget frame</td>
<td>Minimum: 300 pixels, Maximum: Window width, Recommended to adjust based on window size</td>
</tr>
<tr>
<td>global.frameHeight</td>
<td>height of the entire widget frame</td>
<td>Minimum: 480 pixels, Maximum: Window height, Recommended to adjust based on window size</td>
</tr>
<tr>
<td>global.textColor</td>
<td>Color for all texts</td>
<td>Any CSS legal color value. For more information, see CSS Legal Color Values</td>
</tr>
<tr>
<td>global.fontSize</td>
<td>Font size for all texts</td>
<td>Recommended 12 pixels to 20 pixels for different use cases</td>
</tr>
<tr>
<td>global.footerHeight</td>
<td>Height of the widget footer</td>
<td>Minimum: 50 pixels, Maximum: Frame height, Recommended to adjust based on frame size</td>
</tr>
<tr>
<td>header.headerTextColor</td>
<td>Text color for the header message</td>
<td>Any CSS legal color value. For more information, see CSS Legal Color Values</td>
</tr>
<tr>
<td>Custom style name</td>
<td>Description</td>
<td>Recommended constraints</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>transcript.message.FontSize</td>
<td>Font size for all texts</td>
<td>Recommended 12 pixels to 20 pixels for different use cases</td>
</tr>
<tr>
<td>transcript.message.TextColor</td>
<td>Text color for transcript messages</td>
<td>Any CSS legal color value. For more information, see <a href="#">CSS Legal Color Values</a>.</td>
</tr>
<tr>
<td>footer.buttonFontSize</td>
<td>Font size for the action button text</td>
<td>Recommended to adjust based on footer height</td>
</tr>
<tr>
<td>footer.buttonTextColor</td>
<td>Color for the action button text</td>
<td>Any CSS legal color value. For more information, see <a href="#">CSS Legal Color Values</a>.</td>
</tr>
</tbody>
</table>

Following are the elements that make up the communications widget.
Preview your communications widget with custom styles

Make sure to preview your communications widget with the custom styles before putting it into production. Custom values can break the communications widget user interface if not set properly. We recommend testing it on different browsers and devices before releasing it to your customers.

Following are a few examples of things that might break when improper values are used and the suggested fixes.

- **Issue:** The widget window takes up too much of the screen.
  
  **Fix:** Use a smaller frameWidth and frameHeight.

- **Issue:** The font size is too small or too large.
  
  **Fix:** Adjust the font size.

- **Issue:** There is a blank area below end chat (footer).
Fix: Use a smaller frameHeight or a larger footerHeight.

- **Issue:** The end chat button is too small or too big.

  Fix: Adjust buttonFontSize.

- **Issue:** The end chat button is going outside the footer area.

  Fix: Use a larger footerHeight or a smaller buttonFontSize.

**Investigate common issues with adding a chat user interface to your website**

This topic is for developers who need to investigate issues that may occur when configuring a communications widget in the Amazon Connect admin website.

If you see the following **Something went wrong** error message when loading your communications widget, open the browser tools to view the error logs.

Following are common issues that cause this error.

**400 Invalid request**

If the logs mention a 400 invalid request, there are a few possible causes:

- Your communications widget is not being served on an allowed domain. You must specifically state the domains where you will host your widget.

- The request to the endpoint is not properly formatted. This usually occurs only if the contents of the embed snippet have been modified.
401 Unauthorized

If the logs mention a 401 unauthorized, this is a problem with the JSON Web Token (JWT) authentication.

After you have the JWT, you need to implement it in the authenticate callback function. The following example shows how to implement it if you're trying to fetch your token and then use it:

```javascript
amazon_connect('authenticate', function(callback) {
    window.fetch('/token').then(res => {
        res.json().then(data => {
            callback(data.data);
        });
    });
});
```

Here is a more basic version of what needs to be implemented:

```javascript
amazon_connect('authenticate', function(callback) {
    callback(token);
});
```

For instructions on implementing JWT, see [Step 3: Confirm and copy communications widget code and security keys](#).

If you have implemented the callback already, the following scenarios may still cause a 401:

- Invalid signature
- Expired token

404 Not found

A 404 status code indicates that your widgetId cannot be found. Verify that your snippet is exactly how it was copied from the Amazon Connect website, and none of the identifiers have changed.

If the identifiers have not changed and you are seeing a 404, contact AWS Support.
500 Internal server error

This can be caused by your service-linked role not having the required permissions to start chat. This happens if your Amazon Connect instance was created before October 2018 because you don’t have service-linked roles set up.

**Solution:** Add the `connect:*` policy on the role that is associated with your Amazon Connect instance. For more information, see [Use service-linked roles for Amazon Connect](#).

If your service-linked role has the correct permissions, contact AWS Support.

## Create quick responses for use with chat contacts

Quick responses provide contact center agents with pre-written responses that they can use during chat contacts. Quick responses are especially useful for answering common customer inquiries. They help improve agent productivity, reduce handle times, and improve customer satisfaction scores.

You can use the Amazon Connect admin website or [Amazon Q in Connect actions](#) to create quick responses. You can add single quick responses or import many of them at the same time. You can also personalize responses with [user-defined attributes](#). In addition, you can assign shortcut keys to quick responses, and associate them with [routing profiles](#) so that agents can quickly access relevant content.

By default, CCP enables agents to search quick responses. Custom builders can use [Amazon Connect Streams](#) to programmatically implement quick response search in their implementations of CCP.

For information about how agents search for quick responses, see [Search for quick responses in CCP](#).

### Contents

- [Assign permissions to manage quick responses](#)
- [Set up an Amazon Q in Connect knowledge base to store quick responses](#)
- [Add quick responses for use with chat contacts](#)
- [Add attributes for personalizing quick responses](#)
- [Edit quick responses](#)
• **Delete quick responses**
• **Import quick responses**
• **View import history**
• **Enable quick responses in a custom CCP**

**Assign permissions to manage quick responses**

To create and manage quick responses in the Amazon Connect admin website, users need the Content Management security profile permissions. The following image shows these permissions on the Security profiles page.

Following is a description of the Content Management permissions.

- **All** – Enables all permissions, but you must have a custom view to enable **Access**.
- **Access** – Grants users access to custom views. This checkbox remains unavailable until you create a custom view.
- **Create** – Enables users to create Amazon Q in Connect knowledge bases and quick responses in the Amazon Connect admin website. This setting also enables users to View and Edit. It does not grant permission to delete quick responses.
- **View** – Enables users to view quick responses in the Amazon Connect admin website.
- **Edit** – Enables users to edit quick responses in the Amazon Connect admin website.
- **Delete** – Enables users to delete quick responses in the Amazon Connect admin website.

If you want the same users to add personalized attributes to quick responses, they will also need the **Channels and flows, Flows - Publish** permission.
For information about adding permissions to an existing security profile, see Update security profiles.

Set up an Amazon Q in Connect knowledge base to store quick responses

You must create an Amazon Q in Connect knowledge base to store quick responses. You can use the Amazon Connect admin website to create the knowledge base with a single click. The site uses AWS owned keys to encrypt data.

Note
You can create your own key by providing a custom ServerSideEncryptionConfiguration in an CreateKnowledgeBase API call. For more information, see Enable Amazon Q in Connect for your instance, in this guide.

The following steps explain how to use the Amazon Connect admin website to create an Amazon Q in Connect knowledge base.

To create a knowledge base

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
   Use an admin account, or an account with Content Management - Quick responses - Create permission in its security profile.
2. On the navigation bar, choose Agent applications, then Quick responses.
3. On the Quick responses page, choose Get started.

Note
If the Get started button isn't available, sign in with an account that has the admin security profile, or ask another admin for help.

4. Remain on the page until the process ends. Do not refresh the page until the process ends. An indicator shows the status.
The finished knowledge base provides two sample quick responses.

- The sample responses are associated with the **basic routing profile**, if that exists in your Amazon Connect instance.
- The sample responses are set to **Inactive**, meaning agents can't see or search for them. Activating a sample quick response makes it visible and searchable by agents assigned to the basic routing profile.
- If the basic routing profile is not present in your Amazon Connect instance, the sample quick responses are associated with **All** routing profiles. After you activate a sample quick response, all agents can see and search for that response, regardless of their assigned routing profiles.

⚠️ Note

Quick responses are only available in the **Chat** channel.

### Add quick responses for use with chat contacts

This topic explains how to add a quick response by using the Amazon Connect admin website. To create a quick response programmatically, see [CreateQuickResponse](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_CreateQuickResponse.html) in the Amazon Q in Connect API Reference.

**To add responses**

1. Log in to the Amazon Connect admin website at `https://instance name.my.connect.aws/`. Use an **Admin** account, or an account assigned to a security profile that has **Content Management - Quick responses - Create** permission.
2. On the navigation bar, choose Agent applications, then Quick responses.

![Agent applications]

3. On the Quick responses page, choose Add response.

![Quick responses]

**Note**

If the Add response button isn't available, sign in with an account that has the admin security profile, or ask another admin for help.

4. On the Add response page, enter a name, description, and shortcut key for the quick response. You must enter a unique name and shortcut key because agents will search on those values.

5. Open the Routing profiles list and select one or more profiles. You can select a maximum of 50 profiles, or choose All. Only the agents assigned to a given profile can see the quick responses associated with that profile.

6. (Optional) Choose Activate: Make this response visible for agents if you want agents to see and search for the response.

7. In the Content section, enter the response, then choose Save.

**Note**

If you configured user-defined attributes in the flow block, those attributes, such as customer name, appear when an agent searches for a response in CCP. For more information, see Set contact attributes.
Add attributes for personalizing quick responses

You can personalize quick responses by adding user-defined attributes. To do so, you use the Amazon Connect admin website to create responses that include Amazon Connect contact attributes. You can also use the Set contact attributes block to create user-defined attributes in flows.

When quick responses contain user-defined attributes, the value of those attributes, such as customer name, appear when an agent searches for a response in CCP.

The following steps explain how to add user-defined attributes to quick responses. You first create a set-contact attribute, and then you add the attribute to a quick response.

To create a set-contact attribute

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Flows - Edit or Create permissions.
2. On the navigation bar, choose Routing, then Flows.
3. On the Flows page, the Type column lists each type of flow. Choose the flow that you want to add attributes to.
4. Follow the steps in Creating a set contact attribute.

Note

In the contact attribute configuration, select the User defined namespace, then save and publish the flow.

5. When finished, complete the next set of steps.

You can follow these steps when creating or updating a quick response.
To add an attribute to a quick response

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Content Management - Quick responses - Create or Edit permission.

2. On the left navigation bar, choose Agent applications, then Quick responses.

3. Choose Add response to create a response.

—or—

Select the checkbox next to the quick response that you want to personalize, then choose Edit.

4. Choose the content section, enter the quick response content, then use handlebar syntax to enter a user-defined attribute. Make sure you include the Attributes namespace prefix. For example, {{Attributes.name_of_your_destination_key}}.

5. Choose Save.

The following steps explain how to test attributes in CCP.

To test attributes

1. Log in to the Amazon Connect admin website chat testing page at https://instance name.my.connect.aws/test-chat.

2. Choose the flow with the user-defined attribute.

3. Start a chat and enter /#searchText, where searchText is the assigned shortcut key.
Edit quick responses

This topic explains how to use the Amazon Connect admin website to edit a quick response. To edit a quick response programmatically, see UpdateQuickResponse in the Amazon Q in Connect API Reference.

To edit a response

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Content Management - Quick responses - Edit permission.

2. On the navigation bar, choose Agent applications, then Quick responses.

3. On the Quick responses page, choose the name of the quick response that you want to edit. You can also select the checkbox next to the response, then choose Edit.

4. As needed, change the following fields:

   - Name
   - Description
   - Shortcut key
   - Routing Profiles
Delete quick responses

This topic explains how to use the Amazon Connect admin website to delete a quick response. To delete a quick response programmatically, see `DeleteQuickResponse` in the *Amazon Q in Connect API Reference Guide*.

⚠️ Important

- You can't undo a deletion.
- Agents can't see or use deleted quick responses.

To delete a response

1. Log in to the Amazon Connect admin website at `https://instance name.my.connect.aws/`. Use an `Admin` account, or an account assigned to a security profile that has `Content Management - Quick responses - Delete` permission.
2. On the navigation bar, choose `Agent applications`, then `Quick responses`.
3. On the `Quick responses` page, select the checkbox next to the response that you want to delete. You can select a maximum of 20 responses.
4. Choose **Delete**.

   A success message appears:

   ![Successfully Deleted selected Quick response.]

   **Note**

   - If the **Delete** button is inactive, sign in to an Amazon Connect an account that has the required security profile, or ask another admin for help.
   - Remain on the page until the delete operation finishes.

**Import quick responses**

You can import a maximum of 100 quick responses at a time from a .csv file. This topic explains how to use the Amazon Connect admin website to import quick responses. To import quick responses programmatically, see [StartImportJob](#) in the *Amazon Q in Connect API Reference*.

**To import responses**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an **Admin** account, or an account assigned to a security profile that has **Content Management - Quick responses - Create** permission.
2. On the navigation bar, choose **Agent applications**, then **Quick responses**.
3. On the **Quick responses** page, choose **Import**.

4. In the **Import** dialog box, choose the **Responses Import Template.csv** link, then save the resulting **Response Import Template.csv** file to your desktop. The file opens in Microsoft Excel or a similar spreadsheet program.

5. In the .csv file, enter values in each column. Remember the following:

   - The **Name** and **Shortcut key** values must be unique across all the quick responses in your Amazon Connect instance.
   - Values in the **Routing Profile** column are case sensitive and must match the name of your routing profile exactly.
   - Do not rename or change the values in the first row of the .csv file. Those header keys are reserved and used to generate payloads for the [CreateQuickResponse](#) API.
   - Remove all instances of `<*Required field>` from the .csv file. They're only for information.

6. Save the .csv file, return to the Amazon Connect admin website, and in the **Import** dialog box, choose **Upload file**.

7. Locate and open the .csv file, then choose **Import**.

   Success or failure messages appear when the import operation finishes. If the operation fails, choose the **Download failed imports link** in the message. Check the .csv file for leading or trailing spaces, and for any messages about the error.

You can navigate away from the **Quick response** page before the import job finishes. Choose the **View import history** link, located below the list of responses, to view status of your import jobs.
View import history

Amazon Connect retains import history for the lifetime of your knowledge base. To delete that history, you must use the `DeleteKnowledgeBase` action to delete the knowledge base.

This topic explains how to use the Amazon Connect admin website to view import histories. To view import histories programmatically, see `ListImportJobs` in the `Amazon Q in Connect API Reference`.

To view import history

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has Content Management - Quick responses - View permission.

2. On the left navigation bar, choose Agent applications, then Quick responses.

3. On the Quick responses page, choose the View import history link.

Enable quick responses in a custom CCP

To enable quick responses for an embedded or custom CCP, you use the Amazon Connect Streams library on GitHub to call the `SearchQuickResponse` API and return a list of quick response search results to CCP. For more information, see Amazon Connect Streams Documentation on Github.
Enable text formatting for your customer's chat experience

With Amazon Connect message formatting, you can enable your customers and agents to quickly add structure and clarity to their chat messages.

You can provide the following types of formatting on both the chat user interface and the agent application using markdown:

- **Bold**
- **Italic**
- **Bulleted list**
- **Numbered list**
- **Hyperlinks**
- **Emoji**
- Attachments. To enable attachments, follow [Enable attachments to share files using chat and upload files to cases](#).

How to enable message formatting

1. When you create a new chat user interface, rich text formatting is enabled out of the box. No additional configuration is required.
2. To add text formatting capabilities to an existing chat user interface, update the communications widget code with the following code that is highlighted in bold:

```javascript
(function(w, d, x, id){
    s=d.createElement('script');
    s.src='https://d3xxxx.cloudfront.net/amazon-connect-chat-interface-client.js';
    s.async=1;
    s.id=id;
    d.getElementsByTagName('head')[0].appendChild(s);
    w[x] = w[x] || function() { (w[x].ac = w[x].ac || []).push(arguments) };
})(window, document, 'amazon_connect', 'widget-id');

amazon_connect('styles', { openChat: { color: 'white', backgroundColor: '#123456' }, closeChat: { color: 'white', backgroundColor: '#123456' } });
amazon_connect('snippetId', 'snippet-id');
amazon_connect('supportedMessagingContentTypes', [ 'text/plain', 'text/markdown' ]);,
```

The code that is highlighted in red is set to the correct values when you get the snippet from the Amazon Connect console. The only content you choose to add or remove is the last line in bold for supportedMessagingContentTypes.

3. To add text formatting capabilities to your own custom chat user interface (for example, Chat Interface or your own UI solution on top of ChatJS), follow these steps:

   a. Call the StartChatContact API. When calling StartChatContact, add the SupportedMessagingContentTypes parameter as shown in bold in the following example:

   ```javascript
   // Amazon Connect StartChatContact API
   {
       "Attributes": {
           "string" : "string"
       },
       "ClientToken": "string",
       "ContactFlowId": "your flow ID",
       "InitialMessage": {
           "Content": "string",
           "ContentType": "string"
       },
   }
   ```
b. Import `chatjs` as an object, as shown in the following example:

```javascript
import "amazon-connect-chatjs";

this.session = connect.ChatSession.create({
  ...
});

this.session.sendMessage({
  message: "message-in-markdown-format",
  contentType: "text/markdown"
});
```

If you don't use ChatJs, see these topics for information about sending markdown text through Amazon Connect APIs: [StartChatContact](#) and [SendMessage](#).

c. Send messages with markdown. See the previous code snippet for importing `chatjs` as an object for an example of how to send messages. You can use simple markdown for formatting text in chats. If you’re already using chatjs today to send plaintext messages you can modify your existing logic to call `SendMessage` with `text/markdown` as `contentType` instead of `text/plain` when you want to send markdown messages. Be sure to update the `sendMessage` parameter to have the markdown format of your messages. For more information, see [Markdown Guide Basic Syntax](#).

d. Implement your own logic in the UI package to render markdown messages in the input area and chat transcript. If you use React, you can use [react-markdown](#) as a reference.

### Note
- Text formatting capabilities appear to your agent only if the feature has been enabled for your customer in the chat user interface. If text formatting is not supported or enabled
on the customer chat user interface, the agent will not have the ability to compose and send messages with text formatting.

- All text formatting capabilities except attachments are available for quick responses.

Enable message *Delivered* and *Read* receipts in your chat user interface

You can enable message *Delivered* and *Read* in your chat user interface so your customers know the status of the messages they send. This provides transparency to customers, and improves the overall chat experience.

⚠️ **Tip**

By default message receipts are already enabled in the Test chat experience, the Contact Control Panel (CCP), and downloadable open source example of the chat widget.

To enable message receipts in your chat user interface

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Choose Customize communications widget.

2. Choose Edit.
3. By default Message receipts is not enabled. Set to Enabled.

Message receipts are now enabled. Customers who are using the communications widget will start seeing Delivered and Read receipts immediately.

**Set up chat timeouts for chat participants**

When a chat conversation between an agent and a customer has been inactive (no messages sent) for a certain amount of time, you may want to consider a chat participant to be idle, and you may even want to automatically disconnect an agent from the chat.

To do this you can configure both idle timeouts and auto-close timeouts using the `UpdateParticipantRoleConfig` action.

**Tip**

You configure chat timeouts for when customers are interacting with Lex, in the Flow block: Get customer input block. See the Configurable time-outs for chat input during a Lex interaction section.
You can set four different types of timers.

- You specify the amount of time that has to elapse before an action is taken.
- Any combination of timers can be used.

<table>
<thead>
<tr>
<th>Timer</th>
<th>Action at end of timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer idle timeout</td>
<td>Mark the customer as idle.</td>
</tr>
<tr>
<td>Customer auto-disconnect timeout</td>
<td>Automatically disconnect the agent from the chat due to customer idleness.</td>
</tr>
<tr>
<td>Agent idle timeout</td>
<td>Mark the agent as idle.</td>
</tr>
<tr>
<td>Agent auto-disconnect timeout</td>
<td>Automatically disconnect the agent from the chat due to agent idleness.</td>
</tr>
</tbody>
</table>

Specify all timers in minutes.

- Minimum: 2 minutes
- Maximum: 480 minutes (8 hours)

Timers apply to participant roles, and apply for life of the chat.

- You configure timers for participant roles such as agent and customer, rather than individual participants.
- After you set the timers, they apply for the life of the chat. If a chat is transferred, the timers apply to the new agent/customer interaction.

How chat timers work

Timers behave as follows:

- Timers run only when both an agent and a customer are connected to the chat.
- Timers are first started when an agent joins the chat, and are stopped if the agent leaves the chat.
• Idle timers run before auto-disconnect timers, if both are configured for a role. For example, if both timers are configured, then the auto-disconnect timer starts only after a participant is deemed idle.

• If only one type of timer is configured for a role, then that timer starts immediately.

• If at any time a participant sends a message, the timers for that participant are reset. If they were considered idle, they will no longer be.

• The configuration that was set when the agent joined applies for as long as the agent remains on the chat. If you update the timer configuration while an agent and customer are already connected to each other, the new configuration is stored but not applied until and unless a new agent connects to the chat.

• When an auto-disconnect event occurs, all participants other than the customer (such as the agent and any monitoring supervisor) are disconnected. If a Set disconnect flow block has been configured, the chat is routed to it.

**Messages displayed to participants**

Messages are displayed to all participants when any one of the following events happen:

• A participant becomes idle.

• An idle participant sends a message, and is no longer idle.

• An auto-disconnect occurs. Because the agent is disconnected, they won't be able to see the message.

These events are not persisted to the transcripts, nor billed.

The default messages (in all supported languages) are displayed to agents in the Contact Control Panel (CCP) for each of these events.

The following image show examples of default idleness messages that the agent would see in the CCP. For example, *Agent has become idle.*
Recommended usage

To use the chat timeout feature, we recommend that you do the following:

1. Embed a call to the `UpdateParticipantRoleConfig` action in a Lambda in a contact flow.
2. Depending on your use case, place the Lambda either immediately after starting the chat (at the beginning of the flow) or right before routing the contact to a queue.

Customize the customer's chat user interface for a disconnect event

To customize your customer's chat user interface for a disconnect event, see the following methods in the `ChatJS`:
• `onParticipantIdle(callback)`
• `onParticipantReturned(callback)`
• `onAutoDisconnection(callback)`

Use these methods to register callback handlers which are triggered when the new events arrive.

**Enable persistent chat**

Customers often start a chat, then leave the conversation and return later to continue chatting. This may happen many times over the course of several days, months, or even years. To support long running chats like these, you enable persistent chat.

With persistent chat, customers can resume previous conversations with the context, metadata, and transcripts carried forward. Customers don't need to repeat themselves when they return to a chat, and agents have access to the entire conversation history.

**Chat rehydration**

Persistent chat is achieved through a process called chat rehydration, this process enables chat transcripts to be retrieved from previous chat contacts and displayed, allowing customers and agents to easily continue conversations from where they left off.

⚠️ **Important**

Only chat sessions that have ended are allowed to rehydrate onto a new chat session.

Amazon Connect supports two types of rehydration:

• **ENTIRE_PAST_SESSION**: Starts a new chat session and rehydrates all chat segments from past chat sessions.
• **FROM_SEGMENT**: Starts a new session and rehydrates from the specified past chat segment.

For example use cases that show these different rehydration modes, see [Example use cases](#).

**RelatedContactId**

A new contact can have an association with an existing contact through the `RelatedContactId`. This new contact contains a copy of the [contact properties](#) from the related contact.
For more information about how the RelatedContactId is modeled in contact records, see Contact records data model.

For persistent chat, the RelatedContactId depicts the contactId used to source chat rehydration.

**How to enable persistent chat**

To enable persistent chat, you can either specify a previous contact ID when creating a new chat or you can add the Create persistent contact association block to a contact flow.

**Note**

You can choose either method, noted below, to persist chats but not both. That is, you can only enable persistence of a SourceContactId on a new chat once.

To deliver persistent chat experiences you need to provide a previous contact ID when starting a new chat or when using the Create persistent contact association flow block. This is not automatically done for you. It is recommended that you create a repository for storing CTR data, which will enable retrieval of this data for each of your customers. This can be done using chat message streaming to create an entry when a chat has ended or alternatively by inspecting Contact events and using AWS Lambda function for creating entries into your repository. After a repository is setup you can retrieve the previous contact ID for the customer and provide it when starting a new chat or within the Create persistent contact association flow block.

In addition, please ensure past chat transcripts can be retrieved from your instance's Amazon S3 bucket. Using multiple chat transcript buckets or changing the chat transcript file name that is generated by Amazon Connect will prevent retrieval of transcripts, and will not allow chats to persist.

**Enable Persistent chat when creating a new chat contact**

To set up persistent chat experiences when creating a new chat contact, provide the previous contactId in the SourceContactId parameter of the StartChatContact API, this will enable the chat transcripts of previous contacts to be “rehydrated” and shown to both the customer and agent within the chat UI’s, see Example use cases.
Enable Persistent chat within a contact flow

To setup persistent chat experiences within a contact flow, after a chat contact has been created, add the Create persistent contact association block to your contact flow and programmatically specify a source contact ID by using a user defined attribute. You can also use the new CreatePersistentContactAssociation API and provide a source contact ID to make the current chat persistent. For more information, see CreatePersistentContactAssociation in the Amazon Connect API Reference.

Example use cases

For example, a customer starts a chat session:
1. Agent a1 accepts the chat, and the conversation starts between the customer and agent a1. This is the first contact created in the current chat session. For example, the contactId C1 might be 11111111-aaaa-bbbb-1111-1111111111111.

2. Agent a1 then transfers the chat to Agent a2. This creates another contact. For example, contactId C2 might be 2222222-aaaa-bbbb-2222-222222222222222.

3. Agent a2 ends the chat.

4. The customer is forwarded to the disconnect flow for a post-chat survey that creates another contact. For example, contactId C3 might be 33333333-aaaa-bbbb-3333-3333333333333.

5. The post-chat survey is displayed, and the chat session ends.

6. Later, the customer returns and wants to resume their past chat session.

At this point, there are potentially two different use cases for the customer. Following are the persistent chat use cases the customer can have, and how you configure Amazon Connect to provide them.

Use case 1

The customer wants to continue their past chat session but they want to hide the post-chat survey. You use the following configuration to provide this experience.

Request:

```
PUT /contact/chat HTTP/1.1
Content-type: application/json
{
    "Attributes": {
        "string" : "string"
    },
    "ContactFlowId": "string",
    "InitialMessage": {
        "Content": "string",
        "ContentType": "string"
    },
    "InstanceId": "string",
    ... // other chat fields

    // NEW Attribute for persistent chat
    "PersistentChat": {
        "SourceContactId": "2222222-aaaa-bbbb-2222-222222222222222",
        "RehydrationType": "FROM_SEGMENT"
    }
}
```
Configuration

- SourceContactId = 2222222-aaaa-bbbb-2222-222222222222222 (the contactId for C2)
- RehydrationType = "FROM_SEGMENT"

Expected behavior

- This configuration starts a persistent chat session from the specified past ended contact C2 (for example, 2222222-aaaa-bbbb-2222-222222222222222).

  Transcripts of past chat sessions C2 (2222222-aaaa-bbbb-2222-222222222222222) and C1 (11111111-aaaa-bbbb-1111-111111111111111) are accessible in the current persistent chat session. Note that chat segment C3 (33333333-aaaa-bbbb-3333-3333333333333) is dropped from the persistent chat session.

- In this case, the StartChatContact response returns C2 (2222222-aaaa-bbbb-2222-222222222222222) as "ContinuedFromContactId".

- The RelatedContactId for this persistent chat session is 2222222-aaaa-bbbb-2222-222222222222222 (C2).

Use case 2

The customer wants to continue the past chat session and see the transcript of the entire past engagement (and they don’t want to hide the post-chat survey). You use the following configuration to provide this experience.

Note

For the ENTIRE_PAST_SESSION rehydration type, specify the first contact (initial contactId) of the past chat session as the SourceContactId attribute.

Request:

PUT /contact/chat HTTP/1.1
Content-type: application/json
Configuration

- SourceContactId = 11111111-aaaa-bbbb-1111-1111111111111 (C1)
- RehydrationType = "ENTIRE_PAST_SESSION"

Expected behavior

- This starts a persistent chat session from the most recently ended chat contact (C3). Transcripts of past chat sessions C3, C2 and C1 are accessible in the current persistent chat session.
- In this case, the StartChatContact response returns 33333333-aaaa-bbbb-3333-3333333333333 (C3) as "ContinuedFromContactId".
- The RelatedContactId for this persistent chat session is 33333333-aaaa-bbbb-3333-3333333333333 (C3)

Note

Chat linkages are cumulative. After chat sessions are linked, they carry over.
For example, if a contact (contactId C2) that belongs to a past chat session was linked to a contact (contactId C1) from a different past chat session, then a new persistent chat
session created by linking C2 results in implicit linkage of C1 as well. The new persistent chat session will have the following linkage: C3 → C2 → C1

The past contactId, which the persistent chat session is continued from, is exposed in the ContinuedFromContactId field in the StartChatContact API response. It's also in the RelatedContactId field in the contact record for the contact.

How to access past chat contact transcript for a persistent chat

Accessing the past chat transcript for persistent chat uses the existing NextToken pagination model. The initial call to GetTranscript on a newly started persistent chat session contains a NextToken in the response, if past chat messages exist. NextToken must be used to access the past chat transcript along with setting the ScanDirection to BACKWARD on the subsequent GetTranscript call to fetch past chat messages.

If there are multiple past chat messages, GetTranscript returns a new NextToken and the same process can be repeated to fetch more past chat transcripts.

Not supported: using StartPosition and contactId filters for persistent chat

Amazon Connect does not support using StartPosition and contactId filters on the GetTranscript call for transcript item attributes that are from the past chat.

Enable Apple Messages for Business

Note

Temporary unavailability of Amazon Connect Chat integration with Apple Messages for Business

The Amazon Connect Chat integration with Apple Messages for Business is currently unavailable to new customers. This temporary pause is part of our ongoing efforts to enhance the capabilities of the integration.

Your customers can engage directly with your contact center from within their Messages application on their iPhone, iPad, and Mac.

When you enable Apple Messages for Business, your customers can find answers to their questions and request help from agents to resolve issues — all while using the familiar Messages application.
they use every day to chat with friends and family. Any time customers use Search, Safari, Spotlight, Siri, or Maps to call your registered phone number, they will be provided with the option to chat with your contact center.

Apple Messages for Business integration with Amazon Connect enables you to use the same configuration, analytics, routing, and agent UI that you already use for Amazon Connect Chat.

**Step 1: Register with Apple**

Integrate Apple Messages for Business with Amazon Connect by first registering with Apple as a brand. When you do, you'll get a unique Apple Messages for Business Account ID, and you can then link your Apple Messages for Business account to Amazon Connect.

1. Go to the [Apple Messages for Business](https://messages.apple.com/business) page. In the box that says **As a business, I want to connect with my customers in the Messages app**, choose **Get Started**.
2. Create an Apple ID for your business, if you don't already have one.

   An Apple ID is typically for the personal use of Apple services, such as storing personal content in iCloud and downloading apps from the App Store. If you have a personal Apple ID, we recommend that you create a separate one using your organization's email address to administer Messages for Business. A separate administrative Apple ID lets you distinguish Messages for Business communications from personal Apple communications.

3. Register a profile for a new Messages for Business account by accepting **Apple's Terms of Service**. We recommend creating a [Commercial Messages for Business Account](https://developer.apple.com/business/messaging/articles/commercial-messages-business-settings). You then provide business details, such as a logo and support hours.

4. Select Amazon Connect as your Messaging Service Provider. You can do this by selecting Amazon Connect from the drop-down or by entering the following URL:

   - [https://messagingintegrations.connect.amazonaws.com/applebusinesschat](https://messagingintegrations.connect.amazonaws.com/applebusinesschat)

After you submit your application to Apple, you'll see the status of your application at the top of your [Messages for Business Account](https://messages.apple.com/business) page.

For more information about registering with Apple, see the following articles on Apple's website: [Getting Started with Messages for Business](https://developer.apple.com/business/messaging/articles/getting-started) and [Messages for Business Policies and Best Practices](https://developer.apple.com/business/messaging/articles/policies).

**Step 2: Gather required information**

Gather the following information so you have it on hand when you open a support ticket in Step 3:
1. **Apple Messages for Business Account ID**: After you’ve been approved by Apple Messages for Business, you will be issued an Apple Messages for Business Account ID. For information about locating your Apple Messages for Business Account ID, see [Find your Apple Messages for Business Account ID](#).

    ⚠️ **Note**
    
    Your Apple Messages for Business Account ID is a randomized string of numbers and letters. It is not the same as your Apple ID.

2. **Apple Token**: This is a unique ID that authenticates your account. For help locating your Apple token, see [Find your Apple token](#).

3. **Amazon Connect instance ARN**: This is the identifier for the instance you want to link to your Apple business account. For information about locating your instance ID, see [Find your Amazon Connect instance ID/ARN](#).

    ⚠️ **Note**
    
    Make sure you have service-linked roles enabled for the integration.
    
    If your instance was created before **October 2018**, add the `connect:*` policy on the role that is associated with your Amazon Connect instance. For more information about service-linked roles, see [Use service-linked roles for Amazon Connect](#).

4. **Amazon Connect flow ID**: This is the identifier for the flow you want to use for inbound chats. For information about locating your flow ID, see [Find the flow ID](#).

**Step 3: Link your Apple Messages for Business ID to Amazon Connect**

In this step you create an Amazon Connect support ticket to link your Apple Messages for Business ID to Amazon Connect.

1. Create a [special AWS Support ticket](#) to link your Apple Messages for Business to Amazon Connect.

    If prompted, login using your AWS account.
2. Choose **Account and billing**.

3. Use the dropdown box to choose **Account**. For **Category** choose **Activation**, and then choose **Next step: Additional information**.

4. For **Subject** enter **Apple Messages for Business Integration request**.

5. In the **Description** box, copy and paste the following template:

   ```
   Subject: Apple Messages for Business Integration request  
   Body:  
   Apple Messages for Business Account ID (required): *enter your account ID*  
   Apple Token (required): *enter your Apple token*  
   Amazon Connect Instance ARN (required): *enter your instance ARN*  
   Amazon Connect Flow ID (required): *enter your flow ID*
   ```

   The following image shows an example of a completed ticket:
6. Choose **Next step**.

7. Choose **Contact us**, choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.

8. Choose **Submit**.
9. AWS Support will work directly with the Amazon Connect team on your request and follow up with any additional questions.

Next steps

After Apple Messages for Business is enabled for your Amazon Connect instance, you can add Apple Messages for Business features to your messages. For example:

- Deflect calls with Apple's Message Suggest.
- Embed Apple Messages for Business buttons on your website.
- Add list pickers, time pickers, and quick replies to your messages.
- Use rich links for URLs.
- Route Apple Messages for Business messages using contact attributes.

Send a test message for Apple Messages for Business

After onboarding to the Apple Messages for Business account, use the following steps to send a test message to make sure the integration is set up properly.

Step 1: Add internal testers to your Messages for Business account

1. Sign in to Apple Business Register.
2. Choose Messages for Business Accounts and select the account to add testers.
3. Scroll down the page to Account Testing.
4. Add the Apple IDs of your internal testers.
5. When your list is complete and you are ready to begin testing, choose Send to new testers to send an instructional email to your testers.

An instructional email containing a link to your Messages for Business conversation is sent to the Apple ID email address of each tester. If a tester does not receive the email, then recheck that their email address is provided in the Account Testing section. It's most likely that the email address is incorrect or it's not an Apple ID. For security reasons, Apple cannot verify Apple ID email addresses.
Step 2: Test sending and receiving messages

When your testers get the instructional email, they will need to activate the link in it. After doing this, they can send messages to your agents, who can then reply from the Contact Control Panel (CCP).

Note the following:

1. Design a test to trigger all of your Apple Messages for Business features.
2. You should observe that messages sent from an iOS device arrive to your test business. Employees testing from your support agent desktop should be able to respond to these test messages.
3. Your testers may notice your brand colors are not visible in the Messages header. Brand color is not available while your account is in test mode. The colors for your brand will display correctly after your account goes online.
4. If you send the testing link to someone whose email is not listed in the Account Testing section, they will not be able to send messages.
5. If you provide a Redirect Page URL and your testers try to enter Messages for Business from an unsupported device, they will land either on a default or redirected page. You can set your Redirect Page URL in the Unsupported Devices section at the bottom of your Messages for Business account page.

To begin testing

1. Check that your testers are using a device with a supported iOS: iOS 11.3 and later, or macOS 10.13.4.
2. Ask your testers to doing the following:
   a. Use their supported devices to find the email sent to them.
   b. Open the email from the supported device, and then choose the link. It takes them to a Messages for Business conversation in the Messages app.

Troubleshoot

If you encounter any issues when sending a test message, follow these steps:
1. Confirm that you’ve allowlisted your email address/Apple ID as a tester in your Messages for Business account.

2. Confirm the following settings on your Apple device:
   - Go to **Settings > Messages** and check that **iMessage** is enabled.
   - Go to **Settings > Messages > Send & Receive** and check that the AppleID is correct and messages are allowed to receive.

3. Check that you're using a supported iOS. Apple devices running iOS 11.3 and later or macOS 10.13.4 and later support Messages for Business.

4. When you selected Amazon Connect as your MSP in your Apple Account, did you select **Amazon Connect** from the dropdown? Or did you enter the following URL:
   - https://messagingintegrations.connect.amazonaws.com/applebusinesschat

   If you entered the URL, doublecheck for typos.

Add Apple Messages for Business features

**Deflect calls with Apple's Message Suggest**

With **Message Suggest** you can allow users to choose between voice and messaging when tapping on your business phone number in Safari, Maps, Siri, or Search.

To enable Message Suggest, send an email to the Apple Messages for Business Team at **registry@apple.com** with the following information and Apple can set up the channel for you:

- Provide all of your primary phone numbers, including high call volume phone numbers.
- Provide phone contact hours to set customer expectations for your after-hours message.
- Provide intent, group, and body parameters to associate with each phone number.
- Provide an estimate of how many customers your agents can support per day. This can be increased or decreased depending on operational capacity.

To learn more about enabling Message Suggest, see [Apple’s Message Suggest FAQs](#).

**Embed Apple Messages for Business buttons**

To embed Apple Messages for Business buttons on your website or mobile app, do the following:
1. Add Apple's Messages for Business JS (JavaScript) library to your webpage headers.
2. Add a div container to house the button.
3. Customize the banner, fallback support, and button color to meet your brand's needs.

The Messages for Business button must contain the following, at minimum:

- A class attribute to specify the type of container: banner, phone, or message.
- A data-apple-business-id attribute with the business ID you received when you registered your company with Messages for Business.

**Start a chat from a URL**

You can give your customers the ability to start a conversation with you from your website or an email message.

For example, customers may start a chat using a URL that you provide. When they click the URL, the system redirects them to Messages so they can send your business a text message.

You decide how and where to provide the URL. You can include it as a link in an email message, on your website, or use it as the action for a button in your app.

Use the URL **https://bcrw.apple.com/urn:biz:** your-business-id, replacing your-business-id with the business ID you received from Apple after registering with Messages for Business.

Following are optional query string parameters you can include in the URL:

- biz-intent-id: Use to specify the intention, or purpose, of the chat.
- biz-group-id: Use to indicate the group, department, or individuals best qualified to handle the customer's specific question or problem.
- body: Use to prepopulate the message so the customer only presses Send to start the conversation.

Following is an example of what the URL might look like for a customer with a credit card question for the billing department:

Add list pickers, time pickers, and quick replies

A list picker prompts your customer to select an item, such as a product or the reason for their inquiry. A time picker prompts your customer to choose an available time slot, such as to schedule an appointment. A quick reply prompts your customer to select a simple, inline response.

For information about how to set up list pickers, time pickers, and quick replies, see Add interactive messages to chat.

Use rich links for URLs

Rich links show an inline preview of a URL that contains an image. Unlike normal URLs, customers can view the image immediately in a chat without choosing a "Tap to Load Preview" message.

To learn more about Apple Messages for Business rich links, see Rich Links on the Apple Developer website.

Requirements for using rich links in Amazon Connect

To use rich links in Amazon Connect chat messages, your URL and images must meet the following requirements:

- Your website must use Facebook Open Graph tags. For more information, see A Guide to Sharing for Webmasters.
- The image accompanying the URL must be .jpeg, .jpg, or .png.
- The website must be HTML.

Note

When you first use the rich link feature, we recommend that you send the URL in a message separate from your chat text, as shown in the following example. The first message introduces the URL. The next message includes the URL.
Use Apple Messages for Business contact attributes in contact flows

Contact attributes enable you to store temporary information about the contact so you can use it in the flow.

For example, if you have different lines of business using Apple Messages for Business, you can branch to different flows based on the **AppleBusinessChatGroup** contact attribute. Or, if you want to route Apple Messages for Business messages differently from other chat messages, you can branch based on MessagingPlatform.

For more information about contact attributes, see [Use Amazon Connect contact attributes](#).

Use the following contact attributes to route Apple Messages for Business customers.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessagingPlatform</td>
<td>The messaging platform from where the customer request originated.</td>
<td>User-defined</td>
<td>$.Attributes.MessagingPlatform</td>
</tr>
<tr>
<td></td>
<td>Exact value: <strong>AppleBusinessChat</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppleBusinessChatCustomerId</td>
<td>The customer’s opaque ID provided by Apple. This remains constant for the AppleID and a business. You can use this to identify if the message is from a new customer or a returning customer.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatCustomerId</td>
</tr>
<tr>
<td>AppleBusinessChatIntent</td>
<td>You can define the intent or purpose of the chat. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the <strong>Business Chat</strong> button.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatIntent</td>
</tr>
<tr>
<td>AppleBusinessChatGroup</td>
<td>You define the group which designates the department or individuals best qualified to handle</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatGroup</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSON</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>the customer’s particular question or problem. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the Business Chat button.</td>
<td>JSON</td>
<td></td>
</tr>
<tr>
<td>AppleBusinessChatLocale</td>
<td>Defines the language and AWS Region preferences that the user wants to see in their user interface. It consists of a language identifier (ISO 639-1) and a Region identifier (ISO 3166). For example, en_US.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatLocale</td>
</tr>
<tr>
<td>AppleTimePickerCapability</td>
<td>Whether the customer device supports time pickers. If true, customer device supports. If false, their device does not supports.</td>
<td>User-defined</td>
<td>$.Attributes.AppleTimePickerCapability</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSON</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>AppleListPickerCapability</td>
<td>Whether the customer device supports list pickers.</td>
<td>User-defined</td>
<td>$.Attributes.AppleListPickerCapability</td>
</tr>
<tr>
<td></td>
<td>If true, customer device supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If false, their device does not supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppleQuickReplyCapability</td>
<td>Whether the customer device supports quick replies.</td>
<td>User-defined</td>
<td>$.Attributes.AppleQuickReplyCapability</td>
</tr>
<tr>
<td></td>
<td>If true, customer device supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If false, their device does not supports.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Update an Apple Messages for Business integration**

You will need to update your Apple Messages for Business integration if you want to change the flow ID or other information.

1. Open an [AWS Support ticket](https://aws.amazon.com/support/tickets/).
   
   If prompted, login using your AWS account.

2. In the **Use case description** box, copy and paste the following template to indicate this is an update request:

   **Subject:** Update Apple Messages for Business Integration request
   **Body:**
   - Apple Messages for Business Account ID (required): *enter your current account ID* change to *new account ID*
   - Apple Token (required): *enter your token*
Amazon Connect Instance ARN (required): enter your current instance ARN change to new instance ARN
Amazon Connect Flow ID (required): enter your current flow ID change to new flow ID

Note
If you update your Amazon Connect Instance ARN, you must also update your contact flow ID.

3. Expand Contact options, and then choose your Preferred contact language, and then choose Web as the contact method, if it's not selected by default.

4. Choose Submit.

5. AWS Support will work directly with the Amazon Connect team on your request and follow up with any additional questions.

Delete an Apple Messages for Business integration

1. Open an AWS Support ticket.

   If prompted, log in by using your AWS account.

2. In the Use case description box, copy and paste the following template to indicate this is an delete request:
Subject: Delete Apple Messages for Business Integration

Body:

Apple Messages for Business Account ID (required): enter your account ID
Amazon Connect Instance ARN (required): enter your instance ARN
Amazon Connect Flow ID (required): enter your flow ID

The following image shows an example of a completed ticket:

3. Expand **Contact options**, and then choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.

![Contact options](image)

4. Choose **Submit**.

5. **AWS Support** will work directly with the **Amazon Connect team** on your request and follow up with any additional questions.

**Find your Apple Messages for Business Account ID**

1. In **Apple Business Register**, navigate to **Message Service Provider** and click or tap **Test your Messaging Service Provider connection**.
2. Click or tap **Copy ID**.
Find your Apple token

Find the flow ID

The flow ID is the flow you want to use for inbound Apple Messages for Business messages. Flows define the experiences for your customer when they begin a new chat.

You can either reuse an existing flow that you're already using for voice or chat contacts, or create a new one specifically for Apple Messages for Business contacts. For instructions about creating a new inbound flow, see Create an inbound flow.

For more information about flows, see Create Amazon Connect Flows.

To find your flow ID for Apple Messages for Business

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to view contact flows.
2. On the navigation menu, choose Routing, Contact flows.
3. Select the flow you want to use.

Note

Only choose flows that are type Flow (inbound). Apple Messages for Business doesn't work with other flow types, such as Customer queue, Customer hold, Customer whisper, etc.

4. In the flow designer, expand Show additional flow information.
5. Under the ARN (Amazon Resource Number), copy everything after contact-flow/. For example, in the following image, you would copy the underlined part.

1. Notice the **Type = Flow (Inbound)**.
2. The flow ID is at the end of the ARN. Only copy this end part.

**Manage Apple Messages for Business chats**

When you integrate Apple Messages for Business with your Amazon Connect instance, messages from Apple Messages for Business behave exactly like any other chat messages arriving to your contact center.

---

**Note**

The Amazon Connect Chat service quota limits apply to Apple Messages for Business. To learn more, see [Amazon Connect service quotas](#).

---

**Set up automatic replies**

You can use Amazon Lex to set up automatic replies to chat. For a tutorial that introduces you to setting up Amazon Lex and Amazon Connect, see [Add an Amazon Lex bot to Amazon Connect](#).

**Enable real-time chat message streaming**

Amazon Connect Chat provides [APIs](#) that enable you to subscribe to a real-time stream of chat messages. Using these APIs, you can:

- Stream chat messages in real time when a new chat contact is created.
- Extend the current Amazon Connect Chat functionality to support use cases like building integrations with [SMS solutions](#) and third-party messaging applications (for example, [Facebook Messenger](#)), enabling mobile push notifications, and creating analytics dashboards to monitor and track chat message activity.

**How the message streaming APIs work**

The [Amazon Connect message streaming APIs](#) are triggered when certain events occur within an Amazon Connect Chat contact. For example, when a customer sends a new chat message, the event sends a [payload](#) to a specified endpoint containing data about the message that was just sent. Messages are published using [Amazon Simple Notification Service](#) (Amazon SNS) to a specific endpoint.
This topic describes how to set up real-time message streaming using Amazon Connect and Amazon SNS. The steps are:

1. Use the Amazon SNS console to create a new standard SNS topic and set up the messages.
2. Call the StartChatContact API to initiate the chat contact.
3. Call the StartContactStreaming API to initiate message streaming.
4. Call the CreateParticipantConnection API to create the participant's connection.

**Step 1: Create a standard SNS topic**

1. Go to the Amazon SNS console.
2. **Create a SNS topic** in your AWS account. In the Details section, for Type, choose Standard, enter a name for the topic, and then choose Create topic.

   Note: Currently, the message streaming APIs only support standard SNS for real-time streaming of messages. They don't support Amazon SNS FIFO (first in, first out) topics.

3. After you create the topic, its Amazon Resource Name (ARN) is displayed in the Details section. Copy the topic ARN to the clipboard. You'll use the topic ARN in the next step, and in **Step 3: Enable message streaming on the contact**.

   The topic ARN looks similar to the following example:

   arn:aws:sns:us-east-1:123456789012:MyTopic

4. Choose the Access policy tab, choose Edit, and then add a resource-based policy on the SNS topic so that Amazon Connect has permission to publish to it. Following is a sample SNS policy that you can copy and paste into the JSON editor, and then customize with your values:

   ```json
   {
   "Version":"2012-10-17",
   "Statement":[
   {
   "Effect":"Allow",
   "Principal":{
```
Note

The default **Access policy** comes with conditions applied to `sourceOwner` such as:

```
"Condition": {
    "StringEquals": {
      "AWS:SourceOwner": "921772911154"
    }
}
```

Make sure you remove it and replace with `SourceAccount`, for example:

```
"Condition":{
    "StringEquals":{
      "aws:SourceAccount":"YOUR_AWS_ACCOUNT_ID"
    },
    "ArnEquals":{
      "aws:SourceArn":"YOUR_CONNECT_INSTANCE_ARN"
    }
}
```

This prevents a *cross-service confused deputy* issue.

5. If you're using server-side encryption on SNS, verify you have `connect.amazonaws.com` permission enabled on the KMS key. Following is a sample policy:
Step 2: Initiate the chat contact

1. Call the Amazon Connect StartChatContact API to initiate the chat contact.

   For information about how to create the SDK client for calling Amazon Connect APIs, see the following topics:

   - Class AmazonConnectClientBuilder
   - Creating Service Clients

2. Keep track of ContactId and ParticipantToken from the StartChatContact response since these response attributes are used for calling other chat APIs required to enable streaming. This is described in the next steps.

Step 3: Enable message streaming on the contact

- Call StartContactStreaming to enable real-time message streaming to your SNS topic.

  - Limits: You can subscribe to up to two SNS topics per contact.
  
  - When you call StartContactStreaming, you'll need to provide the Amazon Resource Name (ARN) of the SNS topic (see Step 1: Create a standard SNS topic).

    A single SNS topic ARN may be used across multiple AWS accounts, but it must be in the same Region as your Amazon Connect instance. For example, if your topic ARN is in us-east-2, your Amazon Connect instance must be in us-east-2.

    - For initial chat messages that aren't received on the streaming endpoint, you can call the GetTranscript API to receive the initial messages.

Step 4: Create the participant connection

- Call CreateParticipantConnection with the ConnectParticipant attribute passed as true.

  - You must call CreateParticipantConnection within five minutes of creating the chat.
  
  - Calling CreateParticipantConnection with ConnectParticipant set to true only works if you enabled streaming in Step 2: Initiate the chat contact and caller participant is Customer.

  - This step (creating the participant connection) is optional if you have already successfully connected to the chat contact using WEBSOCKET.

Enable real-time message streaming
**Next steps**

You are all set for working with the message streaming APIs.

1. To verify it is working, check that messages are published to the SNS topic you created. You can do this using Amazon CloudWatch metrics. For instructions, see [Monitoring Amazon SNS topics using CloudWatch](#).

2. Because SNS has **limited retention**, we recommend that you set up Amazon Simple Queue Service (Amazon SQS), Amazon Kinesis, or another service to retain messages.

3. Using **StopContactStreaming** is optional and not required if the chats are being disconnected through a contact flow, or if the customer disconnects the chat. However, StopContactStreaming provides the option to stop the message streaming on the SNS topic, even if the chat is active and ongoing.

**Amazon SNS payload used in message streaming**

After you’ve enabled message streaming successfully, you may need to filter the message to send it to the intended participant: agent, customer, or all.

To filter by participant, read the specific SNS headers attribute—MessageVisibility—to determine whether the message is intended for customer-only, agent-only, or all.

- To send to the customer only: For all code that faces the customer, clients need to filter out messages intended for the customer and build the following logic for forwarding the message to them.

  ```java
  if ( ( MessageVisibility == CUSTOMER || MessageVisibility == ALL) && ParticipantRole != CUSTOMER )
  ```

- To send to the agent only:

  ```java
  if ( ( MessageVisibility == AGENT || MessageVisibility == ALL) && ParticipantRole != AGENT )
  ```

You can also leverage the filtering capability in Amazon SNS by building custom **subscription filtering policies**. This offloads the message filtering logic from the SNS topic subscriber to the SNS service itself.
Message attributes in the payload

Following is a description of each message attribute in the Amazon SNS payload:

- **InitialContactId**: The initial contact ID of the chat.
- **ContactId**: The current contact ID of the chat. The InitialContactId and ContactId can differ if there has been new agent in the chat or the queue-to-queue contact flow.
- **ParticipantRole**: The participant who sent the message.
- **InstanceId**: The Amazon Connect instance ID.
- **AccountId**: The AWS account ID.
- **Type**: Possible values: EVENT, MESSAGE.
- **ContentType**: Possible values: application/vnd.amazonaws.connect.event.typing, application/vnd.amazonaws.connect.event.participant.joined, application/vnd.amazonaws.connect.event.participant.left, application/vnd.amazonaws.connect.event.transfer.succeeded, application/vnd.amazonaws.connect.event.transfer.failed, application/vnd.amazonaws.connect.message.interactive, application/vnd.amazonaws.connect.event.chat.ended, and more.
- **MessageVisibility**: Possible values: AGENT, CUSTOMER, ALL.

Example SNS payload

```json
{
    "Type" : "Notification",
    "MessageId" : "cccccccccccccccccccccccccccccccccccccccccc",
    "Message" : "{"AbsoluteTime":"2021-09-08T13:28:24.656Z","Content":"help","ContentType":"text/plain","Id":"333333333-be0d-4a44-889d-d2a86fc06f0c","Type":"MESSAGE","ParticipantId":"bbbbbbbb-c562-4d95-b76c-dcbca8b4b5f7","DisplayName":"Jane","ParticipantRole":"CUSTOMER","InitialContactId":"33333333-abc5-46db-9ad5-d772559ab556"},"ContactId":"33333333-abc5-46db-9ad5-d772559ab556"",
    "SignatureVersion" : "1",
    "Signature" : "examplegggggg/1tEBYdiVDgJgBoJUniUFcArLFGfg5JCvp0r/v6LPCHiD7A0BWy8+ZoGTMoJBMn80U9jSzYhKbHDbQHaNYTo9sRyQA31JtHHiIseQeMfTDPcaAXqfs8hdIXq4XZaJYqDFqo+/tL+kk85syW/2yyjykDYoUb+dyRGkqMy4aKA22Upfid0tdAZ/GGtXaXSBqazZTEUuSEzt0duLtFntQiYJanU05gtDig==",
```
Troubleshoot issues with message streaming

Messages are not getting published to SNS

When this happens, we recommend checking the information in Step 1: Create a standard SNS topic:

- Make sure you are using standard SNS and not Amazon SNS FIFO (first in, first out). Currently, the message streaming APIs support only standard SNS for real-time streaming of messages.
- Make sure an SNS resource-based permission is applied correctly in your account.
  - If server-side encryption is enabled, you need to give the same Amazon Connect service principal permission for encrypt and decrypt.

Flow doesn't start

If you’re using the message streaming APIs in place of websockets, send a connection acknowledgment event; see Step 4: Create the participant connection. This is synonymous to connecting to websocket. The flow begins only after that the connection acknowledgement event.

Call CreateParticipantConnection after StartContactStreaming to mark Customer as connected; see Step 3: Enable message streaming on the contact. This ensures messages are sent after you have confirmed that the customer is ready to receive them.
Issue not resolved?

If after trying the previous solutions you still have issues with message streaming, contact AWS Support for help.

Amazon Connect administrators can choose one of the following options to contact support:

- If you have an AWS Support account, go to [Support Center](https://support.amazon.com) and submit a ticket.
- Otherwise, open the [AWS Management Console](https://console.aws.amazon.com) and choose Amazon Connect, Support, Create case.

It is helpful to provide the following information:

- Your contact center instance ID/ARN. To find your instance ARN, see [Find your Amazon Connect instance ID/ARN](https).
- Your Region.
- A detailed description of the issue.

Customize chat flow experiences by integrating custom participants

You can integrate other solutions, such as bots, with Amazon Connect chat to create customized chat flow experiences.

Following is an overview of how you can customize your chat flow experience. Implement these steps for each chat segment after the chat conversation is started. We recommend adding an [Invoke AWS Lambda function](https) block to call the APIs in your chat flow.

**Important**

Add a [Play prompt](https) block before a [Invoke AWS Lambda function](https) block. This is required only when an [Invoke AWS Lambda](https) block is the first block in your inbound chat flow.

1. [Enable real-time streaming of chat messages](https).
2. Call the Amazon Connect [CreateParticipant](https) API to add a custom participant (ParticipantRole = CUSTOM_BOT) to the chat contact.
a. For information about how to create the SDK client for calling Amazon Connect APIs, see the following topics:

- Class AmazonConnectClientBuilder
- Creating Service Clients

b. Keep the ParticipantToken that is obtained from CreateParticipant to call CreateParticipantConnection. CreateParticipantConnection returns a ConnectionToken, which you can use to call other Amazon Connect Participant APIs.

When calling CreateParticipantConnection to create a connection for a custom participant:

- Set ConnectParticipant to True to mark the custom participant as connected for message streaming.
- Pass Type as CONNECTION_CREDENTIALS to call the subsequent Amazon Connect Participant Service APIs.
- CreateParticipantConnection should be called within 15 seconds of calling CreateParticipant.

3. After the participant is added to the contact, they can exchange messages with the customer by using Amazon Connect Participant Service APIs.

4. To disconnect the participant, call the DisconnectParticipant API.

**Note**

- A custom participant cannot be added to a chat when an agent or Amazon Lex bot is already present on the contact.
- A custom participant will be disconnected when an agent or Amazon Lex bot joins a contact.
- Only one custom participant can be present on a contact.

We recommend configuring how long a custom participant can chat with a contact:

- Set the Timeout property on the Wait block for the ParticipantRole = CUSTOM_BOT.
If the custom bot participant is not disconnected before the timeout, then the contact is routed down the **Time Expired** branch. This allows you to decide which block to run next to resolve the customer's query.

**Note**

If a contact is routed down the **Time Expired** branch, they are not disconnected from the contact. You must call the [DisconnectParticipant](#) API to disconnect the participant.

**Troubleshooting tip**

If you get a `ResourceNotFoundException` for the custom participant when calling the `CreateParticipantConnection` API, check whether the `CreateParticipantConnection` API was called within 15 seconds of `CreateParticipant` API.

**Set up SMS messaging**

You can enable SMS messaging on Amazon Connect so your customers can text you from their mobile device. With Amazon Lex, you can automate responses to their questions, saving agents valuable time and effort.

This topic explains how to set up and test SMS messaging for Amazon Connect. You use Amazon Pinpoint SMS to procure an SMS-enabled phone number, enable two-way SMS on the number, and then import it into Amazon Connect.

**Contents**

- Step 1: Request a number in Amazon Pinpoint SMS
- Step 2: Enable two-way SMS on the phone number
- Step 3: Update flows to branch on SMS contacts
- Step 4: Test sending and receiving SMS messages
- Next steps
Step 1: Request a number in Amazon Pinpoint SMS

⚠️ Important

Some countries require phone numbers and sender IDs to be registered for use in the country. It can take up to 15 business days to process a registration request after it is submitted. We strongly recommend you begin this process early. For more information about registering, see Registrations. We also strongly recommend reviewing Best practices for requesting SMS numbers before requesting a number.

For instructions for using the CLI to perform this step, see Request a phone number in the Amazon Pinpoint SMS User Guide.

2. In the navigation pane, under Configurations, choose Phone numbers and then Request originator.
3. On the Select country page you must choose the Message destination country from the drop down that messages will be sent to. Choose Next.
4. On the Messaging use case section, enter the following:
   - Under Number capabilities choose either SMS, Voice or both depending on your requirements.

      ⚠️ Important
      
      Capabilities for SMS and Voice can't be changed after the phone number has been purchased.

- **SMS** – Choose if you need SMS capabilities.
- **Voice (text to audio)** – Choose if you need voice capabilities.
- Under Estimated monthly SMS message volume per month – optional choose the estimated number of SMS messages you will send each month.
- For Company headquarters - optional choose either of the following:
• **Local** – Choose this if your company headquarters is in the same country as your customers who will receive SMS messages. For example, you would choose this option if your headquarters is in the United States and your users who will receive messages are also in the United States.

• **International** – Choose this if your company headquarters is not in the same country as your customers who will receive SMS messages.

• For **Two-way messaging** choose **Yes** if you require two-way messaging.

5. Choose **Next**.

6. Under **Select originator type** choose one of the recommended phone number type or one of the available number types. The available options are based on the use case information you filled out in the previous steps.

   • If you choose 10DLC and already have a registered campaign, you can choose the campaign from the **Associate to registered campaign**.

   • If the number type you want isn't available, you can choose **Previous** to go back and modify your use case. Also check the **Supported countries and regions (SMS channel)** to make sure the originator type you want is supported in the destination country.

   • If you want to request a short code or long code, you need to open a case with AWS Support. For more information, see [Requesting short codes for SMS messaging with Amazon Pinpoint SMS](https://aws.amazon.com/documentation/pinpoint/sms/short-code-request/). For more information, see [Requesting dedicated long codes for SMS messaging with Amazon Pinpoint SMS](https://aws.amazon.com/documentation/pinpoint/sms/dedicated-long-code-request/).

7. Choose **Next**.

8. On **Review and request** you can verify and edit your request before submitting it. Choose **Request**.

9. A **Registration Required** window may appear depending on the type of phone number you requested. Your phone number or sender ID is associated with this registration and can't send messages until your registration has been approved. For more information about registrations requirements, see [Registrations](https://aws.amazon.com/documentation/pinpoint/sms/registration/).

   a. For **Registration form name** enter a friendly name.

   b. Choose **Begin registration** to finish registering the phone number or **Register later**.
Important

Your phone number or sender ID can't send messages until your registration has been approved. You are still billed the recurring monthly lease fee for the phone number regardless of registration status.

Step 2: Enable two-way SMS on the phone number

After you have successfully procured a phone number from Amazon Pinpoint SMS, you enable two-way SMS on the phone number with Amazon Connect as the message destination. You can enable two-way SMS messaging for individual phone numbers. When one of your customers sends a message to your phone number, the message body is sent to Amazon Connect.

For instructions for using the CLI to perform this step, see Two-way SMS messaging in the Amazon Pinpoint SMS User Guide.

Note

Amazon Connect for two-way SMS is available in the AWS Regions listed in Chat messaging: SMS subtype.

2. In the navigation pane, under Configurations, choose Phone numbers.
3. On the Phone numbers page choose a phone number.
4. On the Two-way SMS tab choose the Edit settings button.
5. On the Edit settings page choose Enable two-way message, as shown in following image.
6. For Destination type choose Amazon Connect.

7. For Amazon Connect in Two-way channel role choose Choose existing IAM roles.

8. In the Existing IAM roles drop down choose an existing IAM role as the message destination. For example IAM policies, see IAM policies for Amazon Connect in the Amazon Pinpoint SMS User Guide.

   **Tip**
   If you can't create a policy or role, double-check that your Amazon Connect instance is in a Region supported by Amazon Connect SMS.

9. Choose Save changes.

10. In the Import Phone Number to Amazon Connect window:

   a. For the Incoming messages destination drop down choose the Amazon Connect instance that will receive incoming messages.
b. Choose **Import Phone Number**.

11. After the number is successfully imported to Amazon Connect, you can view it in the Amazon Connect admin website: In the left navigation, choose **Channels, Phone numbers**. The SMS number appears on the **Phone numbers** page, as shown in the following image.

![Amazon Connect admin website showing imported SMS number](image)

### Step 3: Update flows to branch on SMS contacts

If you have existing flows that you want to branch when a contact uses SMS, add a **Check contact attributes** block to your flows. This block enables you to send SMS contacts to a specific queue, or take another action.

1. Add a **Check contact attributes** block to your flow, and open the **Properties** page.
2. In **Attribute to check** section, set **Namespace** to **Segment attributes** and **key** to **connect:subtype**.

For more information about Segment attributes, see [SegmentAttributes](#) in the [ContactTraceRecord](#) topic.

3. In the **Conditions to check** section, set **condition** to **Equals** and **value** to **connect:SMS**.

The following image of a **Properties** page shows it's configured to branch when the contact comes in on the SMS channel.

4. Associate the SMS phone number with the flow: In the left navigation, choose **Channels**, **Phone numbers**, choose the SMS number, and then choose **Edit**.
5. Under Flow/IVR, choose the flow you updated, and then choose Save.

Tip
When you first purchase a phone number, the phone number's status is Pending. When the phone number is ready to use, the status is Active. If the phone number
requires registration, then you must complete that step before the phone number’s status changes to Active.

Step 4: Test sending and receiving SMS messages

In this step you use the Contact Control Panel (CCP) and a mobile phone to test sending and receiving SMS messages.

1. In your CCP, set your status to Available.

2. Using a mobile device, send an SMS to the phone number that you requested in Step 1: Request a number in Amazon Pinpoint SMS.

Tip

If your Amazon Pinpoint SMS phone number is still in the SMS sandbox, you can only test sending and receiving SMS messages with verified destination numbers that you have configured. For move instructions, see Moving from the SMS sandbox to production.
Next steps

We recommend the following steps to provide the best experience for your agents and customers.

- **Enable persistent chat**: Customers can resume previous conversations with the context, metadata, and transcripts carried forward. They don’t need to repeat themselves when they return to a chat, and agents have access to the entire conversation history.

- **Create quick responses for use with chat contacts**: Provide agents with pre-written responses to common customer inquiries that they can use while they chat with customers. Quick responses make it faster for agents to respond to customers.

Upgrade to the latest CCP

The URL for the latest Contact Control Panel (CCP) ends with *ccp-v2*

You only need to upgrade to the latest CCP if you’re using one of the following options:

- **The URL for your CCP ends with /ccp#**
- **You use the Amazon Connect Streams API**. The URL associated with *initCCP()* ends with /ccp#

If you’re still unsure whether your using the latest CCP, go to [Compare the earlier and latest CCP](#) to see if your CCP looks like the latest one.

Upgrade on your own schedule, before your automatic upgrade date

To upgrade to the latest CCP before your automatic upgrade date, use the steps in the following sections:

- **My CCP URL ends with /ccp#**
- **I use the Amazon Connect Streams API**

Upgrade later, automatically

If you don’t want to upgrade now, you can choose to wait until your scheduled upgrade date.

Between now and your scheduled upgrade date, we recommend the following change management steps:
• Compare how the upgraded CCP differs from the earlier one. For side-by-side visuals, see Compare the earlier and latest CCP.
• Upgrade your CCP in a test environment. Use the latest CCP to learn how it's different, and to check your configurations.
• Communicate to your agents when the upgrade is going to take place.
• Train your agents to help them get ready.

You can see communications about your auto-upgrade date in the Personal Health Dashboard.

My CCP URL ends with /ccp#

Upgrading to the latest CCP is easy. If you want, you can try out the latest CCP and then at a later date make the switch. Here's what you do:

1. Try it out: Change the URL in your browser from /ccp# to /ccp-v2. The latest CCP appears automatically. If you want, change it back to /ccp# to return to the earlier CCP.
2. Upgrade: Change the URL in your browser from /ccp# to /ccp-v2. Bookmark the URL.
3. If you access the CCP through the Amazon Connect console by choosing the phone icon on the top right of a page, you will be re-directed according to the automatic upgrade date sent by email. Please reach out to your Amazon Solution Architect if your request is more urgent.
4. After the upgrade happens, if you use the /ccp# URL, it resolves to /ccp-v2.

Verify your network settings

We highly recommend setting up your network to use Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.

Using this option helps Amazon Connect Support to quickly troubleshoot any issues you have. Specifically, using *.telemetry.connect.{region}.amazonaws.com passes more metrics to our Support team to help with troubleshooting.
Update your SAML URL to ccp-v2

If you use SAML 2.0 as your identity management system, be sure to update the destination in your relay state URL to **ccp-v2**.

Change destination=/connect/ccp to destination=/connect/ccp-v2.

For more information, see [Use a destination in your relay state URL](#).

**Compare the earlier and latest CCP**

The images in this section show you how the latest CCP differs from the earlier CCP for common tasks that agents perform. The images show both CCP versions in their default state.

---

**Tip**

The chat tab appears on an agent's CCP only if their routing profile includes chat.

---

**Set status, use chat, access quick connects and number pad**

1. Agents use a dropdown to set their status.

![Earlier CCP](https://example.com/earlier CCP)

![Latest CCP](https://example.com/latest CCP)
2. If you have enabled chat for the agent's routing profile, the chat tab appears.

3. Choose the **Quick connects** button to type and call a phone number, or select a quick connect.

4. Choose the **Number pad** button to type and call a phone number. This is useful when the phone number has letters.

**Receive a call**

![Image of call flow](image)

**Earlier CCP**

![Image of call flow](image)

**Latest CCP**

**My CCP URL ends with /ccp#**
Miss a call

Make a call: When to use Quick connects

- Use the Quick connects button to type a number or select a quick connect.
Make a call: When to use Number pad

- Choose the **Number pad** button to type and call a number. This is useful for corporate numbers with letters (for example, 1-800-EXAMPLE).
Make an outbound call

Earlier CCP

Latest CCP
Agent ends a call before being connected to the other party

1. If an agent ends a call before being connected, they are then available for a new contact to be routed to them automatically.
2. If an agent ends a call before being connected, they are prompted to choose **Clear contact**.
Make another call while connected on a call

1. You can see the call that you are on while typing another number or selecting a quick connect.

2. After choosing **Quick connects**, you can choose the **Number pad** button. Then on the **Number pad** page, you can enter a number.
Enter DTMF input while connected on a call

- While on a call, only use **Number pad** to enter DTMF input.
Conference call scenario 1: Leaving a call when one party is on hold and the other is connected

1. Choose **Leave call** to leave the call. This automatically takes the first party off hold and connects them to the second party.

2. If instead you want to end the call, choose the x next to each party's number. This disconnects each party.
Conference call scenario 2: Leaving a call when the other parties are joined

1. Choose **Leave call** to leave the call. The other two parties stay joined.
2. If instead you want to end the call, choose the x next to each party's number. This disconnects each party.
Conference call scenario 3: Leaving a call when the other parties are on hold

1. Choose **Leave call** to leave the call. The other two parties are automatically taken off hold and connected.

2. If instead you want to end the call, choose the x next to each party’s number. This disconnects each party.
Receive a queued callback

![Earlier CCP](image1.png) ![Latest CCP](image2.png)

Miss a queued callback

![Earlier CCP](image3.png) ![Latest CCP](image4.png)
Finish After contact work (ACW)

During After contact work (ACW), agents can finish follow-up work, and then choose **Clear contact**.

I use the Amazon Connect Streams API

**Note**

The Amazon Connect Streams API remains the same between the earlier and latest versions of the CCP. We recommend validating custom implementations built using the Amazon Connect Streams API when upgrading versions to ensure consistency in behavior.

Use the following steps to upgrade to the latest CCP.

1. We recommend using the latest Amazon Connect Streams API.
2. Update the URL associated with `initCCP()` from `/ccp#` to `/ccp-v2`. For information about `initCCP()`, see `connect.core.initCCP()` in the Amazon Connect Streams API documentation on GitHub.
3. Add your domain URL to the Approved origin list:

1. Log in to the [AWS Management Console](https://console.aws.amazon.com/console) using your AWS account.
2. Navigate to the Amazon Connect console.
3. Check that you're in the correct Region for your Amazon Connect instance. Choose your instance.

   ![Amazon Connect virtual contact center instances](image)

4. Choose **Application integration**, and then choose **Add origin**.

   ![Application integration](image)

5. Enter your domain URL. All domains that embed the CCP for a particular instance to be explicitly added. For more information, see [this article](#) on GitHub.

   If you use Salesforce, you need to add the Salesforce domains to your allowlist to prevent any issues with the CTI Adapter CCP functionality. For detailed instructions, see the [Amazon Connect Streams API](#)
Connect CTI Adapter for Salesforce Lightning installation guide or the Amazon Connect CTI Adapter for Salesforce Classic installation guide.

Verify your network settings

We highly recommend setting up your network to use Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.

Using this option helps Amazon Connect Support to quickly troubleshoot any issues you have. Specifically, using *telemetry.connect.{region}.amazonaws.com passes more metrics to our Support team to help with troubleshooting.

Update your SAML URL to ccp-v2

If you use SAML 2.0 as your identity management system, be sure to update the destination in your relay state URL to ccp-v2.

Change destination=/connect/ccp to destination=/connect/ccp-v2.

For more information, see Use a destination in your relay state URL

Provide agents with access to the Contact Control Panel

Note

This is the URL to the CCP website:

- https://instance name.my.connect.aws/ccp-v2/

This is the URL to the agent application:

- https://instance name.my.connect.aws/agent-app-v2/

Steps to ensure agents can access the CCP

Agents use the Amazon Connect Contact Control Panel (CCP) to communicate with contacts. But before agents can access to the CCP and handle contacts, there are a few things you need to do:
1. Ensure your network meets the requirements for using the CCP. For more information see Set up your network.

2. Ensure agents have the appropriate headsets and workstations. For more information see Agent headset and workstation requirements for the CCP.

3. Create a user name and password for agents to log into the CCP, by adding agents to your instance.

4. At minimum, assign them the Agent security profile. This grants them permissions to access the CCP, which they use to manage contacts.

5. Provide the user name, password, and the CCP website link to your agents so they can log in. We recommend telling agents to bookmark the URL to the CCP so they can readily access it.

6. Train your agents on the CCP:
   - Watch Training video: How to use the CCP

Agent application: Everything in one place

Want your agents to manage contacts, and access customer profiles, cases, and knowledge all in one place? Use the agent application!

The agent application is a single web browser interface that hosts the CCP, Customer Profiles, Cases, and Amazon Q in Connect.

If you're using the CCP that is provided with Amazon Connect, after you enable Customer Profiles, Cases, or Amazon Q in Connect, share the following URL with your agents so they can access it in the agent application:

- https://instance name.my.connect.aws/agent-app-v2/

For help finding your instance name, see Find your Amazon Connect instance name.

Grant microphone access in Chrome, Firefox, or Edge

If agents experience problems with their microphone, they may need to grant microphone access in their browser. Choose one of the following articles to get the steps appropriate for your browser:

- Use your camera and microphone in Chrome
• Firefox Page Info window

• How to allow a website to use your camera or microphone while browsing in Microsoft Edge in the article Windows camera, microphone, and privacy

⚠️ Important

A change introduced in Google Chrome version 64 may result in issues with receiving calls if you are using an embedded Contact Control Panel (CCP) softphone using the Amazon Connect Streams library. If you are experiencing issues with your microphone when using Chrome version 64, you can resolve the issue by building and deploying the latest version of the Amazon Connect Streams API, following the steps under Downloading Streams. You can also resolve the issue by using Firefox or Edge as your browser.

How to get help for CCP issues

Agents: Contact your manager or the technical support provided by your company.

Amazon Connect Administrators: See Troubleshooting Issues with the Contact Control Panel (CCP) for detailed troubleshooting steps. Or, log in to the AWS Management Console (https://console.aws.amazon.com/console) using your AWS account. In the upper right corner of the page, choose Support, and open a support ticket.

Agent headset and workstation requirements for the CCP

Agent headsets and workstations in the contact center vary widely. While the Amazon Connect CCP is built to handle high levels of jitter and high latency environments, the architecture of the workstations that agents use, and the location and environment in which they take contacts, can impact the quality of experience.

Headset requirements

The agent's Contact Control Panel (CCP) is compatible with all types of headsets.

For the best agent and customer experience, we recommend using a USB headset.

Alternatively, you can redirect the contact to an external number, in E.164 format, using an agent's existing telephony.
**Note**

If the agent's audio device does not support up to 48khz and the browser asserts a sample rate of 48khz, audio issues such as an audible humming sound may be present in the agent's outgoing audio. This has been seen with Firefox but not with Chrome. For instructions on verifying the sample rate of the agent's headset and browser, see Humming sound in headset: Verify the headset and browser sample rates.

---

**Workstation minimum requirements**

Under-powered workstations can make it difficult for agents to access the tools and resources they need to service contacts. Also, keep in mind the resource requirements when scoping workstations to ensure that they can perform under load while appropriately multitasking for the use case.

Following are the minimum system requirements for the workstations using the CCP only. You'll need to scope additional memory, bandwidth, and CPU for the operating system and anything else running on the workstation to avoid resource contention.

- **Browser**—For a list of all supported browsers, see Browsers supported by Amazon Connect.
- **Network**—100 Kbps bandwidth per connected workstation
- **Memory**—2 GB RAM
- **Processor (CPU)**—2 GHz

**iPhone and other mobile devices are not supported**

The Amazon Connect console, Contact Control Panel (CCP), and agent workspace do not support mobile browsers.

**How to determine whether a workstation is the source of problems**

To determine whether a workstation is the source of problems, you need access to various levels of logging information. However, adding logging and monitoring to workstations that are already experiencing resource contention may further reduce available resources and invalidate test results. We recommended that your workstation meet the minimum requirements, so you leave additional resources available for logging, monitoring, malware scanning, operating system functions, and any other running processes.
Collect additional historical logging and data sources for correlation. If you see a correlation between the time of the event and the time the issue was reported, you may be able to determine the root cause with the following information:

- Round trip time (RTT) and packet loss to endpoints located within your Amazon Connect Region from your agent workstation, or an identical workstation on the same network segment. If no Region endpoints are available because of security policies, any public WAN endpoint suffices, for example, www.Amazon.com. Ideally, use your instance alias address (https://your-instance-alias.my.connect.aws/), and also your signaling address for endpoints.

You can find your Region endpoints here: Amazon Connect endpoints and quotas.

- Regular monitoring of workstations that show processes running, and the current resource usage of each process.

- Workstation performance/utilization in these areas:
  - Processor (CPU)
  - Disk / drive
  - RAM / memory
  - Network throughput and performance

- Monitor all of the preceding for your VDI desktop environment, including RTT/packet monitoring between the agent workstation and the VDI environment.

How to determine whether the agent's headset is the source of the problem

Problems with the agent's headset are usually caused by two issues:

- The connection between the agent's headset and computer.
- The permissions for the browser microphone.

Here's what you need to do:

- **Check that your computer recognizes your headset**—Check the settings in Device Manager to ensure that your computer recognizes the headset and allows proper headset connectivity. For example, if you're using a Windows PC:
  1. Go to Device Manager, then expand Audio inputs and outputs.
2. If your computer recognizes your headset, you'll see it listed there.

- **Check your browser settings for your headset/microphone**
  
  **Chrome**
  
  1. go to **Settings, Site Settings, Microphone**.
  2. Then check that the correct headset is enabled.
  3. To learn more, see **Use your camera and microphone in Chrome**.

  **Firefox**
  
  1. While in the CCP, choose the lock icon in the address bar. If needed, grant permissions to the CCP.
  2. To learn more, see **Firefox Page Info window**.

- **Remove your ad blocker**: If you're using an ad blocker extension, remove it and see if that fixes the problem.

---

⚠️ **Important**

A change introduced in Google Chrome version 64 may result in issues with receiving calls if you are using an embedded Contact Control Panel (CCP) softphone using the Amazon Connect Streams library. If you are experiencing issues with your microphone when using Chrome version 64, you can resolve the issue by building and deploying the latest version of the [Amazon Connect Streams API](https://aws.amazon.com/connect/streams-api/), following the steps under *Downloading Streams*. You can also resolve the issue by using Firefox or Edge as your browser.

---

For more information about solving audio problems, see [Troubleshooting Issues with the Contact Control Panel (CCP)](https://aws.amazon.com/connect/troubleshooting/).

**Problem for agents using the CCP: Can't hear indicator for incoming chat?**

If an agent can't hear the audio indicator for an incoming chat, the problem is likely because Google added an audio policy flag to Chrome. This flag exists in Chrome versions 71 - 75.

To fix this, add the CCP web site to the allowlist in the agent's Chrome settings. For instructions, see this [Google Chrome Help article](https://support.google.com/chrome/answer/95375?hl=en).
For more information about solving audio problems, see Troubleshooting Issues with the Contact Control Panel (CCP).

Embed a custom Contact Control Panel (CCP)

The Amazon Connect Streams documentation describes how to integrate your existing web applications with Amazon Connect. Streams gives you the power to embed the Contact Control Panel (CCP) UI components into your page, and/or handle agent and contact state events directly giving you the power to control agent and contact state through an object oriented event driven interface. You can use the built in interface or build your own from scratch: Streams gives you the power to choose.

Contents

• Use Amazon Connect Streams API for third-party cookies
• Embed the CCP into Salesforce
• Embed the CCP into Zendesk

Use Amazon Connect Streams API for third-party cookies

⚠️ Important

Customers using Amazon Connect Agent Workspace or the Contact Control Panel (CCP) as a standalone application do not need to perform the steps described in this topic.

Amazon Connect uses cookies for authentication. As part of Google’s Privacy Sandbox initiative, Google Chrome has announced plans to block third-party cookies (that is, cookies passed between two top level domains). This topic explains what you need to do to ensure your agents can continue using Chrome with Amazon Connect.

• If you are using custom agent applications with the CCP, Customer Profiles, or Amazon Q in Connect, you must upgrade to the latest available version of the Amazon Connect Streams API. This upgrade prevents the blocking of third-party cookies from impacting Amazon Connect across Chrome and all supported browsers.
• If you are using the Amazon Connect CTI Adapter, you need to upgrade to the latest version of the CTI Adapter (version 5.21 onwards).
We recommend existing customers upgrade to the latest version of the Streams API before the end of 2023. If this is not possible, you can apply a Chrome enterprise policy to enable third-party cookies for your Amazon Connect instance. While a viable interim solution, we recommend that customers still upgrade as soon as possible in case Google does not support this override indefinitely.

Contents

- Agent experience after upgrade
- How to implement the Streams upgrade
- Configure the Grant Access banner for custom CCPs
- Storage access callbacks
- Instructions for testing Google Chrome

Agent experience after upgrade

After you upgrade to the latest version of the Streams API, agents who use custom applications or the CTI Adapter are prompted to allow third-party cookies from Amazon Connect. For example:

1. When agents open the CCP, a new Allow access to cookies banner appears. It has one action button: Grant access.
2. When agents choose Grant access, the browser displays a prompt to authorize the use of third-party cookies.
3. Agents must select Allow on this second pop-up, and then proceed to log in.

Agents may need to renew these permissions if they clear their browser cache, do not interact with the embedded CCP for 30 days, or every 30 days for custom CCPs.

Following are examples of how this experience appears to agents, depending on whether you're using a default or custom configuration of the CCP.

- If you're using the default CCP configuration:
  - Example Grant access banner that is displayed to the agent
Action required!

Allow access to cookies

The Amazon Connect Contact Control Panel (CCP) now requires permissions to access your Amazon Connect login cookies. Choose the Grant access button and use the Allow option. Learn more

Grant access

Example Access denied banner that is displayed to the agent

Action required!

Allow access to cookies

You can't access this website, because you didn't allow access to this website's cookies. Learn more

Try again

If you're using a custom configuration of the CCP, following is an example Grant access banner.

Action required!

Allow access to cookies

As per your browser policy, this website now explicitly requires permission to access cookies. Request access by clicking the below 'Grant Access' button and 'Allow' your browser permissions. This will only allow access to your login cookies. Learn more

Grant access

If desired, you can use Chrome enterprise policies—CookiesAllowedForUrls or BlockThirdPartyCookies—to bypass this Grant access workflow. We recommend that you consult Google's documentation and determine which policy is best for your organization. AWS does not own the behavior of these policies.

What happens if agents don't choose Grant access when prompted?

If agents don't choose Grant access when prompted, they won't be able to log into the CCP. To enable access outside of the login workflow, they will need to do the following steps:
1. Navigate to chrome://settings/content/storageAccess.

2. In the left navigation menu, choose Privacy and security.

3. Choose Third-party cookies.

4. Under You blocked these sites from using info they've saved about you, delete any entries associated with awsapps.com or connect.aws as shown in the following image.

5. You can close that instance of your browser.

6. Open your CCP. When prompted, choose Grant access, and then choose Allow.
How to implement the Streams upgrade

The StreamsJS initCCP method has been updated to load the Request Storage Access banner (RSA banner) before initializing the CCP. Depending on the existing cookie permissions set in the agent's browser, the agent is redirected to either the CCP or the RSA banner.

For implementations that hide the default CCP user interface, you must include new ContainDiv in your custom applications to show the new RSA banner on log in. To do this, pass the mode as custom within the new storageAccess parameter. StreamsJS displays the ContainDiv and then hides it after the process is complete. You can use optional callbacks to hide or show logic as needed, for example, to set the container to a specific height.

- **For custom integrations (using StreamsJS) where the out-of-the-box CCP is visible to agents:** No changes are required on the initCCP parameters.

- **For custom integrations (using StreamsJS) where the out-of-the-box CCP isn't visible to agents:** Configure storageAccess with mode set to custom, as shown in the following code sample. With this configuration, hide or show the ContainDiv by using the display:none or block property in cases where there is custom logic. For example, when using an absolute position to hide the CCP, use Storage access callbacks to add custom logic.

```javascript
connect.initCCP(ContainerDiv, {
    ccpUrl: "https://<alias>.my.connect.aws/ccp-v2",
    "loginPopup": true, // optional
    "loginPopupAutoClose": true,
    "softphone": {
        "allowFramedSoftphone": true
    },

    /**
     * Setting the mode to 'custom' tries to hide or show the ContainDiv based on
     * the cookie permissions
     * if you need any further logic to hide/show the banner, use of callbacks to
     * perform the same
     * For example if you are using margins or positions to hide the div you need
     * to take care of the same
     **/
    "storageAccess": {
        "mode": "custom"
    }
}
```

Use Amazon Connect Streams API for third-party cookies
• **For CTI adapter use cases:** After upgrading to the latest version of the Streams API CTI adapter, no changes are necessary to any adapter configurations or CTI flows.

**Configure the Grant Access banner for custom CCPs**

You can customize the look and feel of the request access banner by using the optional configuration flags shown in the following example.

```javascript
connect.initCCP(ContainerDiv, {
    "ccpUrl": "https://<alias>.my.connect.aws/ccp-v2",
    "softphone": {
        "allowFramedSoftphone": true
    },
    "storageAccess": {
        "canRequest": true, // By default this is set to true. You can set it to false to opt out from checking storage access.
        "mode": "custom",
        /**
         * The following configurations are only used as a sample, please update to use the custom value or remove them completely
         **/
        "custom": {
            "hideCCP": true, // By default this is set to true and is only applicable in "custom" mode. You can set this to false to leave CCPUI visible after granting access in "custom" mode.
            "header": "Action required!",
            "title": "Allow access to cookies",
            "accessBannerDescription": "As per your browser policy, this website now explicitly requires permission to access cookies. Request access by clicking the below ‘Grant Access’ button and ‘Allow’ your browser permissions. This will only allow access to your login cookies.",
            "denyBannerDescription": "You can't access this website because you didn't allow access to this website's cookies.",
            "accessBannerButtonText": "Grant access",
            "denyBannerButtonText": "Try again",
            "accessBannerLearnMoreUrl": "https://wiki.amazon.com/bin/view/access",
            "denyBannerLearnMoreUrl": "https://wiki.amazon.com/bin/view/deny",
            "accessBannerLearnMoreText": "Learn more111",
            "denyBannerLearnMoreText": "Deny learn more123"
        }
    }
});
```
The following values are only used as a sample,
please update to your custom theme or remove them completely
/**
"style": {
"font-family": "sans-serif",
"primary-color": "#007bff",
"primary-button-hover-color": "#034861",
"link-color": "#0078c3",
"banner-header-color": "#212529",
"banner-title-color": "#212529",
"banner-request-access-description-color": "#0c5460",
"banner-request-access-background": "#d1ecf1",
"banner-request-deny-background": "yellow",
"banner-box-shadow": "none",
"banner-margin": "15px",
"border-radius": "0.25rem",
"banner-request-access-icon-color": "#007bff",
"banner-request-deny-icon-color": "green",
"line-height": "25px",
"banner-description-font-size": "14px",
"banner-icon-display": "block",
"header-font-size": "2rem",
"bold-font-weight": "1000"
}
}

Storage access callbacks

You can use the following optional callbacks to handle custom logic for showing and hiding the banner.

```javascript
connect.storageAccess?.onRequest({
onInit: (hasAccess) => {
    // invoked when request access is initialized
    // depending on hasAccess value, you can show the banner within the CCP container
    // for custom CCPs
},
onDeny: () => {
    // after user deny the permission
},
onGrant: () => {
    // after the agent allows the permission, you may want to close the banner
}
```

Use Amazon Connect Streams API for third-party cookies
For the latest technical implementation details for Amazon Connect CCP and the Streams API, see the Amazon Connect Streams API repository.

Instructions for testing Google Chrome

In addition to the following guidance, also refer to this additional resource for testing Google Chrome.

Step 1: Download the correct Chrome version for testing

You can test Chrome's implementation today in Chrome M117. As of September 2023, M117 is available on the Canary channel of Chrome. According to Chrome's published schedule, in the future it will also be available on the Beta and Dev channels.

Step 2: Set required flags in Chrome

Enable flags that Chrome requires by using chrome://flags, as shown in the following image.
Following is a list of the Chrome flags you must enable:

1. Set the `#storage-access-api` flag to **Enabled (with prompt)**.
2. Set the `#permission-storage-access-api` flag to **Enabled**.
3. Set the `#test-third-party-cookie-phaseout` flag to **Enabled**.

**Embed the CCP into Salesforce**

The core functionality of the Amazon Connect CTI Adapter provides a WebRTC browser-based Contact Control Panel (CCP) within Salesforce. The Amazon Connect CTI integration consists of two components:

- **A managed Salesforce package**
• An AWS Serverless application deployed to your AWS environment

For a detailed walk-through and setup of the full CTI Adapter capabilities for Salesforce Lightning, see the Amazon Connect CTI Adapter for Salesforce Lightning installation guide.

For the CTI Adapter for Salesforce Classic, see the Amazon Connect CTI Adapter for Salesforce Classic installation guide.

We recommend that you initially install the package into your Salesforce sandbox. After the package is installed, you can configure your Salesforce Call Center configuration within Salesforce.

**Embed the CCP into Zendesk**

To integrate Amazon Connect and Zendesk, you need:

- An Amazon Connect instance.
- A Zendesk Support account with a Zendesk Talk Partner Edition plan, or a Zendesk trial account.

Install and configure the Amazon Connect for Zendesk app in your Zendesk Support account, then integrate the app with Amazon Connect. After integration, you can create flows to use Amazon Connect with Zendesk ticketing.

For more information, see How do I integrate Amazon Connect with Zendesk?
Set up Amazon Connect Global Resiliency

Note
This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions.
To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

Amazon Connect Global Resiliency enables you to provide customer service anywhere in the world with the highest reliability, performance, and efficiency. With its distributed telephony features, your contact center can meet international regulatory requirements.

Amazon Connect Global Resiliency provides a set of APIs that you use to:

- Provision a linked Amazon Connect instance in another AWS Region.
- Provision and manage phone numbers that are global and accessible in both Regions.
- Distribute telephony traffic and agents across Amazon Connect instances and Regions in 10% increments, or shift them all at once. This enables you to slowly shift inbound voice contacts and agents across Regions or shift them all at the same time.

  For example, you can distribute inbound voice contacts and agents 100% in US East (N. Virginia) and 0% in US West (Oregon), or 50% in each Region.
- Access reserved capacity across Regions.

Contents
- Get started with Amazon Connect Global Resiliency
- Manage traffic distribution groups
- Manage phone numbers across Regions
Get started with Amazon Connect Global Resiliency

- **Note**
  This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions.
  To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

You get started with Amazon Connect Global Resiliency by creating a replica of your existing Amazon Connect instance in another AWS Region, and by creating a traffic distribution group.

A *traffic distribution group* is an Amazon Connect resource that enables you to link Amazon Connect instances that are in different AWS Regions. Phone numbers can be attached to the traffic distribution group. Traffic to these numbers can be distributed between the instances in the traffic distribution group.

### How to set up Amazon Connect Global Resiliency

1. **Create a replica of your existing Amazon Connect instance.** Use the [ReplicateInstance](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/AmazonConnect_ReplicateInstance.html) API.
2. **Create a traffic distribution group.**
   1. Use the [CreateTrafficDistributionGroup](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/AmazonConnect_CreateTrafficDistributionGroup.html) API.
   2. Use [DescribeTrafficDistributionGroup](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/AmazonConnect_DescribeTrafficDistributionGroup.html) API to determine whether the traffic distribution group has been created successfully (*Status* must be *ACTIVE*).
3. **Claim phone numbers to your traffic distribution group.** After your traffic distribution group has been created successfully (*Status* is *ACTIVE*), you can claim phone numbers to it using the [ClaimPhoneNumber](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/AmazonConnect_ClaimPhoneNumber.html) API.

- **Note**
  The default traffic distribution for these phone numbers is set to 100% - 0%. That is, 100% of inbound telephony traffic will go to the source Amazon Connect instance that was used to create a replica.
In addition, after phone numbers are claimed to an instance, you can assign them to multiple instances across AWS Regions. To do this, use the `UpdatePhoneNumber` API to assign the numbers to a traffic distribution group.

4. **Update your traffic distribution.** Use the `UpdateTrafficDistribution` API to distribute traffic across the linked instances in 10% increments.

### Create a replica of your existing Amazon Connect instance

#### Note

This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions. To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

You call the `ReplicateInstance` API to create a replica of your Amazon Connect instance in another AWS Region and to copy configuration information for Amazon Connect resources across AWS Regions.

**Contents**

- **Important things to know**
- **Characteristics of the replica instance**
- **What resources are mirrored in the replica instance**
- **What to do after the replica instance is created**
- **When to contact AWS Support**
- **Why a ReplicateInstance call fails**
- **How to find the source Region of your Amazon Connect instances**

### Important things to know

- Before running `ReplicateInstance:`
• Make sure you have the minimum required IAM permissions to create an instance. See [Required permissions for using custom IAM policies to manage access to the Amazon Connect console](#).

• Ensure your Lambda functions across AWS Regions have the same name.

• Update your flows to replace any hardcoded Regions with a $.AwsRegion or $['AwsRegion'] parameter.

• For Amazon Lex bots, change your flows to branch based on the AWS Region where the flow is running. At flow runtime, these parameters are replaced with the Region where the flow is run.

• **ReplicateInstance** copies the Amazon Connect configuration across AWS Regions as part of the initial replication process. After this first step completes, any changes made to **mirrored resources** at a later time are continuously synchronized to the replica instance across Regions.

• All phone numbers on the source instance that aren't already associated to number groups are automatically added to the default traffic distribution group. This step enables the phone numbers to be available in both source and replica Regions, and enables phone number-flow associations to be mirrored across AWS Regions.

• Emergency access to log into the replica instance is available only after the default routing profile and queue have been mirrored across the Regions.

• As the configuration is propagated across AWS Regions, you can view the progress in AWS CloudTrail logs. Or, in the Amazon Connect admin website you can navigate to **User management, View historical changes** to view an audit trail of changes to the users.

• A resource name conflict will occur if resources in the source instance and the replica instance have the same name but different resource IDs. This might happen, for example, if the resource in the replica instance was created manually outside of the replication process.

  In the case of resource name conflicts, **ReplicateInstance** doesn’t synchronize the resource across Regions. Instead it throws a ResourceConflictException error. After you resolve the name conflict (for example, delete the resource in the replica instance), you can run ReplicateInstance again to synchronize the resource.

• After running ReplicateInstance, you must use the **AssociateTrafficDistributionGroupUser** API to associate agents to either the default traffic distribution group or a custom traffic distribution group.

• Running **ReplicateInstance** does not synchronize Lambda functions or Amazon Lex bots, or other third-party / integrations you may have.
Characteristics of the replica instance

- The replica Amazon Connect instance is created in the same AWS account as your existing Amazon Connect instance.
- `ReplicateInstance` creates a default traffic distribution group if one doesn't already exist. This default traffic distribution group has three types of traffic distribution:
  - Sign in
  - Agent
  - Telephony

Use the `CreateTrafficDistributionGroup` API to create more traffic distribution groups, however, these additional traffic distribution groups are not default traffic distribution groups and thus only support agent and telephony distributions.

- The default traffic distribution group is the only traffic distribution group where you can change the `SignInConfig` distribution. See the `IsDefault` parameter in the `TrafficDistributionGroup` data type.
- You use `SignInConfig` to choose the backend sign-in servers to facilitate the agent signing in to their Amazon Connect instance. For example, if you call `UpdateTrafficDistribution` with a modified `SignInConfig` and a non-default `TrafficDistributionGroup`, an `InvalidRequestException` is returned.
- The replica instance has the same instance ID as the Amazon Connect instance it is replicated from.

What resources are mirrored in the replica instance

`ReplicateInstance` mirrors the following Amazon Connect resources across AWS Regions.

⚠️ Important

The service quotas for these resources are automatically matched across AWS Regions before the resources are mirrored across Regions. To increase any other quota in the replica instance, submit a request.

- Flows
- Flow modules
• Users
• Routing profiles
• Queues
• Security profiles
• Hours of operation
• Quick connects
• Prompts (not including those stored in S3)
• User hierarchies (groups and levels)
• Agent status

ReplicateInstance also replicates the following associations across AWS Regions:

• Phone number to flow
• Queue to routing profile
• User to security profile, routing profile, and user hierarchy
• Routing profiles
• Queue to quick connects
• Queue to hours of operation
• Queue to flow

**What to do after the replica instance is created**

After your replica Amazon Connect instance is created, you need to configure it:

1. Ensure redundancy for front-end and back-end integrations (for example, SSO, Lambda, Lex) across Regions.
2. Make matching manual updates across the linked instances.
3. Use the AssociateTrafficDistributionGroupUser API to associate agents to the default traffic distribution group.

Before you can associate agents to a traffic distribution group, they must be present on both the source and replica instances. You cannot associate users to a traffic distribution group when they are newly added to source instance and not yet in the replica.
When to contact AWS Support

Contact AWS Support for help with the following activities:

- To understand mirroring status beyond what's available in the CloudTrail logs and audit trail in the Amazon Connect admin website.
- To stop replication after it is started.
- To delete your replica instance. You need to disassociate numbers and users from traffic distribution groups. AWS Support needs to delete any snapshots we have created for global configuration management.

Why a ReplicateInstance call fails

A ReplicateInstance API call fails with an InvalidRequestException in the following cases:

1. The Region where you are creating the replica is the same Region as your existing instance.
2. The instance was already replicated as part of a different ReplicateInstance API call.
3. The instance does not have an alias.
4. The instance is not in ACTIVE status.
5. The instance does not have SAML enabled.
6. There is a resource name conflict.

How to find the source Region of your Amazon Connect instances

If you forget which Region is your source Region for your Amazon Connect instances, perform the following steps to find it:

1. Call the ListTrafficDistributionGroups API with your InstanceId.
2. For any traffic distribution group in the response list, the returned InstanceARN includes the source Region. For example in the following ARN, source-region would be the Region of your Amazon Connect instance.

Create traffic distribution groups

You can create a traffic distribution group for your existing Amazon Connect instance by using the `CreateTrafficDistributionGroup` API.

A traffic distribution group is an Amazon Connect resource that enables you to link Amazon Connect instances that are in different AWS Regions. Phone numbers can be attached to the traffic distribution group. Traffic to these numbers can be distributed between the instances in the traffic distribution group.

Important things to know

- When creating a traffic distribution group, it must be created in the source AWS Region. A source Region is the Region where you set up your existing Amazon Connect instance.

- When associating phone numbers to a traffic distribution group:
  - You can associate only phone numbers that are claimed in the source Region.
  - The phone number must be in the same Region as where the traffic distribution group was created.

- You can claim numbers to a traffic distribution group, or get or update traffic distribution for a traffic distribution group only when its status is ACTIVE. Use the `DescribeTrafficDistributionGroup` API to determine whether it has been created successfully (Status must be ACTIVE).

- When you create a replica Amazon Connect instance, a default traffic distribution group is created for it. The default traffic distribution group is the only traffic distribution group where you can change the SignInConfig distribution. See the IsDefault parameter in the `TrafficDistributionGroup` data type. You use SignInConfig to choose which backend sign-in servers are used to facilitate the agent signing in to their Amazon Connect instance. For example, if you call `UpdateTrafficDistribution` with a modified SignInConfig and a non-default `TrafficDistributionGroup`, an InvalidRequestException is returned.

Traffic distribution group statuses

Following is a description of the traffic distribution group statuses:

- CREATION_IN_PROGRESS: Traffic distribution group creation is in progress.
- ACTIVE: Traffic distribution group has been created.
• CREATION_FAILED: Traffic distribution group creation failed.
• PENDING_DELETION: Traffic distribution group deletion is in progress.
• DELETION_FAILED: Traffic distribution group deletion failed.
• UPDATE_IN_PROGRESS: Traffic distribution group update is in progress.

Why a CreateTrafficDistributionGroup call fails

A CreateTrafficDistributionGroup API call fails with an InvalidRequestException in the following cases:

• The ReplicateInstance API was not called before creating a traffic distribution group for the linked instances.
• The CreateTrafficDistributionGroup API was not called in the same Region where the ReplicateInstance API was called. The Region where this API is called must match the Region of the instance that was used to create a replica.

Claim phone numbers to traffic distribution groups

Note
This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions.
To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

After your traffic distribution group is created successfully (Status is ACTIVE), you can use SearchAvailablePhoneNumbers to search for available phone numbers and ClaimPhoneNumber to claim them.

Before you claim a phone number to your traffic distribution group, we recommend using the DescribeTrafficDistributionGroup API to verify the status of the traffic distribution group is ACTIVE. Assigning a phone number to a traffic distribution group that isn't ACTIVE results in ResourceNotFoundException.

You can claim a phone number to a traffic distribution group by providing the traffic distribution group ARN in the TargetArn parameter when calling the ClaimPhoneNumber API. You can also
use the UpdatePhoneNumber API to assign a phone number previously claimed to an instance to a traffic distribution group.

Note
To update the Description field, you must use the Amazon Connect console.

Example workflow

Following is an example workflow to claim phone numbers and use them across multiple AWS Regions:

1. Create a replica of your instance:
   - Call the ReplicateInstance API.

2. Create a traffic distribution group that links these instances together:
   - Call the CreateTrafficDistributionGroup API.

3. Find available phone numbers that can be claimed to your traffic distribution group:
   - Call the SearchAvailablePhoneNumbers API in the Region where the traffic distribution group was created. Provide the traffic distribution group ARN for the TargetArn parameter.

4. In the Region where the traffic distribution group was created, call the ClaimPhoneNumber API:
   a. Provide your traffic distribution group ARN for the TargetArn parameter.
   b. Provide the E164 phone number value that was returned by the SearchAvailablePhoneNumbers API call in step 3.

   A PhoneNumberId and PhoneNumberArn are returned. You can use these values for follow-up operations.

5. Verify that the phone number status is CLAIMED:
   - Call the DescribePhoneNumber API.
(DescribePhoneNumber can also be called in the other Region associated with the traffic distribution group. It will return the same phone number details.)

The phone number can be used by follow-up operations only after its status is CLAIMED.

For a description of possible statuses, see Phone number statuses defined.

6. Repeat steps 3-5 for all phone numbers you need to claim to your traffic distribution group.

7. Perform the following steps to associate flows to phone numbers. Do them in both Regions where the traffic distribution group operates.

These steps ensure your telephony traffic will route correctly to your flows to support your traffic distribution configuration.

a. In your existing Amazon Connect instance in the Region where the traffic distribution group was created, do the following steps:

i. Call ListContactFlows API. Provide the InstanceId that corresponds to the instance that was replicated.

ii. A list of flow ARNs is returned. Use these flow ARNs to associate a flow to a phone number; call the AssociatePhoneNumberContactFlow API.

b. In the replicated Amazon Connect instance in the other AWS Region, do the following steps:

i. Call ListContactFlows API. Provide the InstanceId that corresponds to the instance that was replicated.

ii. A list of flow ARNs is returned. Use these flow ARNs to associate a flow to a phone number; call the AssociatePhoneNumberContactFlow API.

Why a ClaimPhoneNumber call fails

Your ClaimPhoneNumber API call will fail with a ResourceNotFoundException in the following cases:

- The specified traffic distribution group does not exist, the status of the traffic distribution group is not ACTIVE, or you do not have ownership of the traffic distribution group.
• The phone number is not available for claiming. In some cases, a phone number found from SearchAvailablePhoneNumbers may have been claimed by another customer.

ClaimPhoneNumber will fail with an InvalidParameterException error in the following case:

• The endpoint you are calling is not in the same Region where the traffic distribution group was created.

Phone number statuses defined

Following is a description of phone number statuses:

• CLAIMED means the previous ClaimPhoneNumber or UpdatePhoneNumber operation succeeded.

• IN_PROGRESS means a ClaimPhoneNumber, UpdatePhoneNumber operation is still in progress and has not yet completed. You can call DescribePhoneNumber at a later time to verify if the previous operation has completed.

• FAILED indicates that the previous ClaimPhoneNumber or UpdatePhoneNumber operation has failed. It includes a message indicating the failure reason.

A common reason for a failure is that the TargetArn value you are claiming or updating a phone number to has reached its limit of total claimed numbers.

If you received a FAILED status from a ClaimPhoneNumber API call, you have one day to retry claiming the phone number before the number is released back to the inventory for other customers to claim.

Assign claimed phone numbers to traffic distribution groups

• You created a new traffic distribution group and it's status is ACTIVE. We recommend using the DescribeTrafficDistributionGroup API to verify the status.

• You have already claimed phone numbers to instances or other traffic distribution groups.

Now you can assign those claimed phone numbers to your new traffic distribution group by using the UpdatePhoneNumber API. Provide the traffic distribution group ARN in the TargetArn parameter.
Note

To update the Description field, you must use the Amazon Connect console.

Example workflow

Following is an example workflow to assign claimed phone numbers to your traffic distribution group:

1. Call the UpdatePhoneNumber API to assign the phone number to a new TargetArn.

   The TargetArn can be for another Amazon Connect instance or for a traffic distribution group created in the same Region where the phone number was initially claimed.

2. Perform the following steps to associate flows to phone numbers. Do them in both Regions where the traffic distribution group operates.

   These steps ensure your telephony traffic will route correctly to your flows to support your traffic distribution configuration.

   a. In your existing Amazon Connect instance in the Region where the traffic distribution group was created, do the following steps:

      i. Call the ListContactFlows API. Provide the InstanceId that corresponds to the instance that was replicated.

      ii. A list of flow ARNs is returned. Use these flow ARNs to associate a flow to a phone number; call the AssociatePhoneNumberContactFlow API.

   b. In the replicated Amazon Connect instance in the other Region, do the following steps:

      i. Call the ListContactFlows API. Provide the InstanceId that corresponds to the instance that was replicated.

      ii. A list of flow ARNs is returned. Use these flow ARNs to associate a flow to a phone number; call the AssociatePhoneNumberContactFlow API.

Why an AssociatePhoneNumberContactFlow call fails

If the number is claimed to a traffic distribution group, and you are calling AssociatePhoneNumberContactFlow using an instance in the AWS Region where the traffic
distribution group was created, you can use either a full phone number ARN or UUID value for the PhoneNumberId URI request parameter.

However, if the number is claimed to a traffic distribution group and you are calling this API using an instance in the replica AWS Region associated with the traffic distribution group, you must provide a full phone number ARN. If a UUID is provided in this scenario, you will receive a ResourceNotFoundException.

Why an UpdatePhoneNumber call fails

Your UpdatePhoneNumber API call will fail with a ResourceNotFoundException in the following case:

- The specified traffic distribution group does not exist, the status of the traffic distribution group is not ACTIVE, or you do not have ownership of the traffic distribution group.

UpdatePhoneNumber will fail with a InvalidParameterException error in the following case:

- The endpoint you are calling is not in the same Region where the traffic distribution group was created.

Phone number statuses defined

Following is a description of phone number statuses:

- CLAIMED means the previous ClaimPhoneNumber or UpdatePhoneNumber operation succeeded.
- IN_PROGRESS means a ClaimPhoneNumber, UpdatePhoneNumber operation is still in progress and has not yet completed. You can call DescribePhoneNumber at a later time to verify if the previous operation has completed.
- FAILED indicates that the previous ClaimPhoneNumber or UpdatePhoneNumber operation has failed. It includes a message indicating the failure reason. A common reason for a failure is that the TargetArn value you are claiming or updating a phone number to has reached its limit of total claimed numbers.

Update telephony traffic distribution across AWS Regions

You use the UpdateTrafficDistribution API to distribute telephony traffic and shift agents across Regions.
After you have claimed phone numbers to your traffic distribution group, you can use the \texttt{UpdateTrafficDistribution} API to distribute inbound voice contacts across linked instances in a given traffic distribution group in 10% increments.

If the following requirements are not met, your \texttt{UpdateTrafficDistribution} API call will fail with an \texttt{InvalidRequestException}:

- You must provide distribution for telephony traffic configuration.
- You must specify the traffic distribution for both linked instances and the total distribution must add up to 100%.
- You must specify traffic distribution in 10% increments.
- The instance ARNs specified in the telephony configuration must match the ARNs of the linked instances.

When you call \texttt{UpdateTrafficDistribution} from the source AWS Region you can use either the traffic distribution group ID or Amazon Resource Name (ARN). When you call \texttt{UpdateTrafficDistribution} in the replica Region, you must use the traffic distribution group ARN.

\textbf{Set up your agent's experience with Amazon Connect Global Resiliency}

Amazon Connect Global Resiliency enables you to provide a global experience for agents with global sign-in, agent distribution API, and CCP enhancements. With these set of features, you can:

- Enable your agents to sign in once at the beginning of their day and process contacts from their current active Region without needing to know which Region is active at any time.
- Add agents to your traffic distribution group and distribute agents across AWS Regions.
- Redirect new inbound voice contacts to the CCP for the current active Region without needing an action on your agent's part.

\textbf{Contents}

- \underline{Integrate your identity provider (IdP) with a new AWS sign in SAML endpoint}
- \underline{Associate agents to instances across multiple AWS Regions}
- \underline{Update agent distribution across AWS Regions}
- \underline{Set up Streams for embedded and custom CCP}
• Set up Amazon Connect Agent Workspace to support agents shifting across AWS Regions
• The agent's experience with the CCP when shifted across Regions
• Tips for avoiding issues when shifting agents across Regions

Integrate your identity provider (IdP) with a new AWS sign in SAML endpoint

To enable your agents to sign in once and be logged into both AWS Regions to process contacts from the current active Region, you need to configure IAM settings to use the global sign in SAML endpoint.

Before you begin

You must enable SAML for your Amazon Connect instance to use Amazon Connect Global Resiliency. For information about getting started with IAM federation, see Enabling SAML 2.0 federated users to access the AWS Management Console.

Important things to know

• To perform the steps in this topic, you'll need your instance ID. For instructions about how to find it, see Find your Amazon Connect instance ID/ARN.
• You will also need to know the source Region of your Amazon Connect instances. For instructions about how to find it, see How to find the source Region of your Amazon Connect instances.
• Agents must be created already in both your source and replica Amazon Connect instances and have the same username as the role session name from your identity provider (IdP). Otherwise, you will receive a UserNotOnboardedException exception and risk losing agent redundancy capabilities between your instances.
• You must associate agents to a traffic distribution group before agents attempt to sign in. Otherwise agent sign-in will fail with a ResourceNotFoundException exception. For information about how to setup your traffic distribution groups and associate agents to them, see Associate agents to instances across multiple AWS Regions.
• When your agents federate into Amazon Connect with the new SAML sign-in URL, Amazon Connect Global Resiliency always attempts to log the agent into both your source and replica Regions / instances, no matter how SignInConfig is configured in your traffic distribution group. You can verify this by checking CloudTrail logs.
• The SignInConfig distribution in your default traffic distribution group only determines which AWS Region is used to facilitate sign-in. Regardless of how your SignInConfig distribution is
configured, Amazon Connect always attempts to sign in agents to both Regions of your Amazon Connect instance.

- After replicating an Amazon Connect instance, only one SAML sign-in endpoint is generated for your instances. This endpoint always contains the source AWS Region in the URL.
- You don’t need to configure a relay state when using the personalized SAML sign-in URL with Amazon Connect Global Resiliency.

How to integrate your identity provider

1. When you create a replica of your Amazon Connect instance using the `ReplicateInstance` API, a personalized SAML sign-in URL is generated for your Amazon Connect instances. The URL is generated in the following format:

   https://instance-id.source-region.sign-in.connect.aws/saml

   a. `instance-id` is the instance ID for either instance in your instance group. The instance ID is identical in the source and replica Regions.

   b. `source-region` corresponds to the source AWS Region in which the `ReplicateInstance` API was called.

2. Add the following trust policy to your IAM Federation role. Use the URL for the global sign-in SAML endpoint as shown in the following example.

   ```json
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Federated": [
             "saml-provider-arn"
           ]
         },
         "Action": "sts:AssumeRoleWithSAML",
         "Condition": {
           "StringLike": {
             "SAML:aud": [
               "https://instance-id.source-region.sign-in.connect.aws/saml*"
             ]
           }
         }
       }
   }
   ```
3. Grant access to `connect:GetFederationToken` for your `InstanceId` on your IAM Federation role. For example:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GetFederationTokenAccess",
      "Effect": "Allow",
      "Action": "connect:GetFederationToken",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "connect:InstanceId": "your-instance-id"
        }
      }
    }
  ]
}
```

4. Add an attribute mapping to your identity provider application using the following attribute and value strings.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https://aws.amazon.com/SAML/Attributes/Role</code></td>
<td><code>saml-role-arn ,identity-provider-arn</code></td>
</tr>
</tbody>
</table>

5. Configure the Assertion Consumer Service (ACS) URL of your identity provider to point to your personalized SAML sign-in URL. Use the following example for the ACS URL:
6. Set following fields in the URL parameters:

- **instanceId**: The identifier of your Amazon Connect instance. For instructions about how to find your instance ID, see [Find your Amazon Connect instance ID/ARN](#).
- **accountId**: The AWS account ID where the Amazon Connect instances are located.
- **role**: Set to the name or Amazon Resource Name (ARN) of the SAML role used for Amazon Connect federation.
- **idp**: Set to the name or Amazon Resource Name (ARN) of the SAML identity provider in IAM.
- **destination**: Set to the optional path where agents will land in the instance after signing in (for example: /agent-app-v2).

### Associate agents to instances across multiple AWS Regions

To allow your agents to sign-in to both AWS Regions and process contacts from either Region, you must first assign them to a traffic distribution group.

1. If you have not yet set up a traffic distribution group, do so now. For instructions, see [Create traffic distribution groups](#).

2. After your traffic distribution group is created successfully (Status is ACTIVE), you can assign agents to it. Always associate users to a traffic distribution group in the source Region.

   Assigning an agent to a traffic distribution group without an ACTIVE status results in ResourceNotFoundException. Use the [DescribeTrafficDistributionGroup](#) API to determine whether it has been created successfully (Status must be ACTIVE).

3. You can assign an agent to a traffic distribution group by calling the [AssociateTrafficDistributionGroupUser](#) API.

### Examples

The following `associate-traffic-distribution-group-user` example command shows how agents can be associated to and used across multiple AWS Regions.

```bash
aws connect associate-traffic-distribution-group-user
```
The following **AssociateTrafficDistributionGroupUser** example associates an agent with a traffic distribution group.

```bash
PUT /traffic-distribution-group/trafficDistributionGroupId/user HTTP/1.1
Content-type: application/json

{
    "UserId": "string"
}
```

The following **disassociate-traffic-distribution-group-user** example command disassociates an agent from a traffic distribution group.

```bash
aws connect disassociate-traffic-distribution-group-user
--instance-id your instance ID
--traffic-distribution-group-id UUID
--user-id UUID
```

The following **DisassociateTrafficDistributionGroupUser** example disassociates an agent from a traffic distribution group.

```
DELETE /traffic-distribution-group/trafficDistributionGroupId/user/UserId HTTP/1.1
```

**Why an AssociateTrafficDistributionGroupUser call fails**

An **AssociateTrafficDistributionGroupUser** API call fails with an ResourceNotFoundException in the following cases:

1. The specified traffic distribution group does not exist.
2. The status of the traffic distribution group is not ACTIVE.
3. The user-id **UUID** is not a user from the source Amazon Connect instance.
Update agent distribution across AWS Regions

Just as you can use the UpdateTrafficDistribution API to distribute telephony traffic across Regions, you can also use it to distribute agents across AWS Regions, either fully or gradually as part of regular operational readiness testing. For example, you might keep 40% of agents in one AWS Region to complete active contacts and shift the remaining agents to the replica Region.

After you have added agents to your traffic distribution group, use the UpdateTrafficDistribution API to distribute agents across linked instances in a given traffic distribution group in 10% increments. Your agents will be able to complete active voice contacts before shifting Regions.

Note

If an agent gets an error when they try to end a contact before shifting Regions, they need to refresh the CCP page. For more information, see The agent’s experience with the CCP when shifted across Regions.

Contents

• Requirements
• Change sign-in weights
• How to shift all telephony traffic and agents across AWS Regions

Requirements

If the following requirements are not met, your UpdateTrafficDistribution API call will fail with an InvalidRequestException:

1. The specified traffic distribution group must exist.
2. The status of the traffic distribution group must be ACTIVE.
3. If you are changing the SignInConfig distribution, you can only do so for the default traffic distribution group. The default traffic distribution group is created when the replica Amazon Connect instance is created. See the IsDefault parameter in the TrafficDistributionGroup data type.

When you call UpdateTrafficDistribution from the source AWS Region you can use either the traffic distribution group ID or Amazon Resource Name (ARN). When you call
UpdateTrafficDistribution in the replica Region, you must use the traffic distribution group ARN.

**Change sign-in weights**

The UpdateTrafficDistribution API includes a distribution called SignInConfig. It allows you to choose which backend sign-in servers are used to facilitate the agent signing in to their instance group. Regardless of the SignInConfig set in your traffic distribution group, agents will be signed in to both instances in the traffic distribution group.

For the best experience, we recommend having both AWS Regions enabled during regular operations. To achieve this pass `true` to both SignInConfig distributions. If you need to shift your entire telephony traffic and agents across to one AWS Region, we recommend changing the SignInConfig to `false` for the Region you are shifting traffic away from.

For example, the following call results in agents having a 50% chance of using the us-west-2 sign-in server and a 50% of using the us-east-1 sign-in server for a given login call from the identity provider.

```
aws connect update-traffic-distribution \
--id traffic distribution group ID or ARN \
--cli-input-json \
'\n  "SignInConfig":{\n    "Distributions":[\n      {\n        "Region":"us-west-2",\n        "Enabled":true \n      },\n      {\n        "Region":"us-east-1",\n        "Enabled":true \n      }\n    ]\n  }\n'
```

Conversely, the following sign-in distribution routes 100% of traffic on the sign-in endpoint to use the us-east-1 sign-in server.

```
aws connect update-traffic-distribution \
```
This distribution controls only which Region of the sign-in server is used to facilitate logging in the agent to both instances in their instance group. It doesn't affect the distribution of agents controlled by the `AgentConfig` part of the `UpdateTrafficDistribution` API.

⚠️ Important

If the sign-in endpoint is not responsive during agent sign-in and your `SignInConfig` distribution is split across Regions, then you can resolve the errors by changing distribution to a single AWS Region. Or, if your `SignInConfig` is weighted on one Region and it isn't responsive, you can try shifting the `SignInConfig` to the disabled Region. Regardless of how your `SignInConfig` is configured, agents will still benefit from having a session active in both the source and replica Regions because they will attempt to sign into their Amazon Connect instance in both Regions.

**How to shift all telephony traffic and agents across AWS Regions**

To shift all new inbound voice contacts, agent sign-in distribution, and agent distribution from `us-west-2` to `us-east-1`, use the following code snippet.

```bash
aws connect update-traffic-distribution \
--id traffic distribution group ID or ARN \
--cli-input-json \n'{
  "SignInConfig":{
    "Distributions":[
      {
        "Region":"us-west-2",
        "Enabled":false
      },
      {
        "Region":"us-east-1",
        "Enabled":true
      }
    ]
  }
}
'```
When you call UpdateTrafficDistribution from the source AWS Region you can use either the traffic distribution group ID or Amazon Resource Name (ARN). When you call UpdateTrafficDistribution in the replica Region, you must use the traffic distribution group ARN.
Set up Streams for embedded and custom CCP

To enable embedded or custom CCP to redirect new inbound voice contacts to the current active Region for an agent, you need to integrate with the new Amazon Connect Streams library that is specifically designed for use with traffic distribution groups.

- The new Streams library can be used only with Amazon Connect instances that are part of a traffic distribution group.
- It does not replace the existing Streams library (connect-streams.js or connect-streams-min.js) used in single Region Amazon Connect instances that are not part of traffic distribution groups.
- It is the same as the single Region / instance Streams library but instead of embedding only one CCP, you configure information for CCPs corresponding to both source and replica instances in your traffic distribution group.

Additionally, the new Amazon Connect Streams library suppresses contacts from the Amazon Connect instance in the Region where the agent is not currently active. In embedded use cases where the native CCP UI is visible, the Streams library shows only the CCP for the Region where the agent is active. In the event of a change to the agent's active Region, Streams automatically switches the embedded UI to display CCP for the newly active Region, and hides the CCP UI for the Region where the agent was previously active.

By default when you use custom or embedded CCP, agents must set their CCP status to Available after they have shifted across Regions. For custom CCP you can implement logic to automatically set their status to Available in the Region they have been shifted to and to display a message to agents. For more information, see the Global Resiliency/Disaster Recovery Streams page on GitHub.

Set up Amazon Connect Agent Workspace to support agents shifting across AWS Regions

Perform the following steps to enable Amazon Connect Agent Workspace to embed the Contact Control Panel from the replica AWS Region to the source Region, and shift between them as agent's active Region changes.

If you have not yet created a replica of your source Amazon Connect instance or set up a traffic distribution group, see Get started with Amazon Connect Global Resiliency.
1. Go to the AWS Amazon Connect console to retrieve the Access URL for your source instance. Make a note of the URL.

2. In the replica Region, AWS Amazon Connect console to retrieve the Access URL for your replica instance. Make a note of the URL.

3. In the same window for your replica Amazon Connect instance, in the left pane choose Approved origins.

4. Add domain for source instance Access URL, which you noted in step 1.

    **Note**
    Do not include a trailing / in the access URL.

5. Repeat the above steps on your source instance: Go to Approved origins, add the access URL for the replica instance.

    **Note**
    Agents must set their status to Available after they are shifted across Regions.

**The agent's experience with the CCP when shifted across Regions**

When you call the UpdateTrafficDistribution API to shift agents across Regions, following is what agents and contacts experience:

- The CCP waits for any active voice contacts to finish.
- Active chat and task contacts are ended immediately as though the agent has disconnected from the contact. Customers will see a system message that the agent has left the chat. They need to restart a new chat, which is then routed to an agent in the Region they have shifted to.
- After the shift across Regions is completed, the agent's status in the CCP is set to Offline.
- By default when you use custom or embedded CCP, agents must set their CCP status to Available after they have shifted across Regions. For custom CCP you can implement logic to automatically set their status to Available in the Region they have been shifted to and to display a message to agents.
- The CCP does not display any messages notifying agents that they have been shifted across Regions. If desired, you can use Streams to customize the CCP to display a message to agents.
When agents are shifted across Regions, they should see the Region change in 1-2 minutes of you calling the `UpdateTrafficDistribution` API and updating agent distribution across Regions. If they don't see their Region change, they can perform one of the following steps:

- Refresh the CCP page.
- If they have multiple CCP tabs where the CCP is embedded they can close all the tabs and then reopen them.

If agents are on active calls and they get dropped, they should refresh their CCP.

**Note**

When you shift traffic in the traffic distribution group, Admins, supervisors, and other users who are signed in to the Amazon Connect admin website, but who don't use the CCP or Agent Workspace, will not be shifted across Regions automatically. These users must manually navigate to the URL of their Amazon Connect instance in the other Region or sign in again after their traffic distribution group has been updated.

### Tips for avoiding issues when shifting agents across Regions

- Whenever you update the traffic distribution for agents be sure to also update the traffic distribution for inbound voice contacts. Otherwise, you might end up in a situation where one Region is heavy on agents while the other is heavy on telephony traffic.

- Before associating agents to a traffic distribution group, create users with the same username in both the source and replica Amazon Connect instances. Otherwise, when you associate a user to a traffic distribution group but the user with the username does not exist in the replica Region, you will get an `InvalidRequestException` error.

- You must call the [AssociateTrafficDistributionGroupUser](https://docs.aws.amazon.com/connect/latest/APIReference/API_AssociateTrafficDistributionGroupUser.html) API to associate agents to a traffic distribution group in the source Region. If you attempt to do this while in the replica Region, you will get a `ResourceNotFoundException` error.

### Manage traffic distribution groups

The topics in this section describe how to manage traffic distribution groups by using Amazon Connect APIs.
List traffic distribution groups

Use the `ListTrafficDistributionGroups` API to list all traffic distribution groups.

You may want to list traffic distribution groups as a way of determining whether a particular Amazon Connect instance is part of any traffic distribution groups.

Delete traffic distribution groups

Use the `DeleteTrafficDistributionGroup` API to delete a traffic distribution group that is no longer needed.

⚠️ Note

You cannot delete a traffic distribution group if phone numbers are claimed to it. You must first release phone numbers from the traffic distribution group by using the `ReleasePhoneNumber` API. After that, you can delete the traffic distribution group.

You cannot release numbers from a traffic distribution group by using the Amazon Connect console.

Your `DeleteTrafficDistributionGroup` API call will fail with an `ResourceInUseException` if phone numbers are still claimed to the traffic distribution group.

Manage phone numbers across Regions

The topics in this section describe how to manage phone numbers across AWS Regions by using Amazon Connect APIs.

Contents

- Claim phone numbers to instances across multiple AWS Regions
- Move a claimed phone number to multiple instances across AWS Regions
- Release numbers from traffic distribution groups
Claim phone numbers to instances across multiple AWS Regions

Note
This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions. To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

To place or receive calls to a phone number across instances in multiple AWS Regions, you need to claim a phone number to a traffic distribution group.

To claim a phone number to a traffic distribution group

1. Create a traffic distribution group by using the `CreateTrafficDistributionGroup` API.
2. Describe your traffic distribution group by using the `DescribeTrafficDistributionGroup` API to determine whether it has been created successfully (`Status` must be `ACTIVE`).
3. After your traffic distribution group has been created successfully (`Status` is `ACTIVE`), you can claim phone numbers to it by using the `ClaimPhoneNumber` API.

Move a claimed phone number to multiple instances across AWS Regions

Note
This feature is available only for Amazon Connect instances created in the US East (N. Virginia) and US West (Oregon) Regions. To obtain access to this feature, contact your Amazon Connect Solutions Architect or Technical Account Manager.

You can move a phone number that was previously claimed to an instance, and instead assign it to multiple instances across AWS Regions. You do this by assigning the phone number to a traffic distribution group.
**To assign a phone number to a traffic distribution group**

1. Create a traffic distribution group using the [CreateTrafficDistributionGroup](#) API.
2. Describe your traffic distribution group using the [DescribeTrafficDistributionGroup](#) API to determine whether it has been created successfully (Status must be ACTIVE).
3. After your traffic distribution group is created successfully (Status is ACTIVE), you can assign phone numbers that were previously claimed to other instances or other traffic distribution groups. Use the [UpdatePhoneNumber](#) API.

**Release numbers from traffic distribution groups**

To release phone numbers from a traffic distribution group, use the [ReleasePhoneNumber](#) API. The number is released back to inventory for other customers to claim it.

You cannot release numbers from a traffic distribution group by using the Amazon Connect console.
Set up your network

Traditional VoIP solutions require you to allow both inbound and outbound for specific UDP port ranges and IPs, such as 80 and 443. These solutions also apply to TCP. In comparison, the network requirements for using the Contact Control Panel (CCP) with a softphone are less intrusive. You can establish persistent outbound send/receive connections through your web browser. As a result, you don't need to open a client-side port to listen for inbound traffic.

The following diagram shows you what each port is used for.

The following sections describe the two primary connectivity options for using the CCP.

Contents

- **Option 1 (recommended):** Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist
- **Option 2 (not recommended):** Allow IP address ranges
- **About Amazon Connect IP address ranges**
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist

This first option lets you significantly reduce your blast radius.

We recommend trying Option 1 and testing it with more than 200 calls. Test for softphone errors, dropped calls, and conference/transfer functionality. If your error rate is greater than 2 percent, there might be an issue with proxy resolution. If that's the case, consider using Option 2.

To allow traffic for Amazon EC2 endpoints, allow access for the URL and port, as shown in the first row of the following table. Do this instead of allowing all of the IP address ranges listed in the ip-ranges.json file. You get the same benefit using a domain for CloudFront, as shown in the second row of the following table.

<table>
<thead>
<tr>
<th>Domain/URL allowlist</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtc.*,conn ect-telec</td>
<td>Replace <code>region</code> with the Region where your</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>Domain/URL allowlist</td>
<td>AWS Region</td>
<td>Ports</td>
<td>Direction</td>
<td>Traffic</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>-------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>om.*region.*amazonaws.com</td>
<td>Amazon Connect instance is located</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain/URL allowlist</td>
<td>AWS Region</td>
<td>Ports</td>
<td>Direction</td>
<td>Traffic</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>-------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Following is the minimum allowlist for *.my.connect.aws:</td>
<td>Replace <code>myInstanceName</code> with the alias of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>myInstanceName.my.connect.aws/ccp-v2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>myInstanceName.my.connect.aws/api</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>myInstanceName.my.connect.aws/auth/authorize</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.static.connect.aws</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.cloudfront.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Following is the minimum allowlist for *.awsapps.com:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>myInstanceName.awsapps.com/connect/ccp-v2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>myInstanceName.awsapps.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.
<table>
<thead>
<tr>
<th>Domain/URL allowlist</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>com/connect/api</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• myInstanceName.awsapps.com/connect/auth/authorize</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• *.cloudfront.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.telemetry.connect.region.amazonaws.com</td>
<td>Replace <code>region</code> with the location of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>participate.connect.region.amazonaws.com</td>
<td>Replace <code>region</code> with the location of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>*.transport.connect.region.amazonaws.com</td>
<td>Replace <code>region</code> with the location of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.
<table>
<thead>
<tr>
<th>Domain/URL allowlist</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 bucket name.s3.region.amazonaws</td>
<td>Replace <em>Amazon S3 bucket name</em> with the name of the location where you store attachments. Replace <em>region</em> with the location of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>TurnNlb-*elb.region.amazonaws</td>
<td>Replace <em>region</em> with the location of your Amazon Connect instance</td>
<td>3478 (UDP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

To instead add specific endpoints to your allowlist based on Region, see NLB endpoints.
<table>
<thead>
<tr>
<th>Domain/URL allowlist</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBALACCELERATOR</td>
<td>GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)</td>
<td>443 (HTTPS) and 80 (HTTP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

Fully qualified domain names (FQDNs) cannot be changed or customized on a per-customer basis. Instead, use **Option 2 - allow IP address ranges**.

**Note**

If you're using SAML Sign-In to your Amazon Connect instance, add the Global Accelerator domain to your allowlist: *.awsglobalaccelerator.com.

**Tip**

When using rtc*.connect-telecom.region.amazonaws.com, *.transport.connect.region.amazonaws.com, and https://myInstanceName.awsapps.com, in certain proxy applications, web socket handling may impact functionality. Be sure to test and validate before deploying to a production environment.

The following table lists the CloudFront domains used for static assets if you want to add domains to your allowlist instead of IP ranges:
<table>
<thead>
<tr>
<th>Region</th>
<th>CloudFront Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td><a href="https://dd401jc05x2yk.cloudfront.net/">https://dd401jc05x2yk.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d1f0uslnncy85vb.cloudfront.net/">https://d1f0uslnncy85vb.cloudfront.net/</a></td>
</tr>
<tr>
<td>us-west-2</td>
<td><a href="https://d38fzyjx9jg8fj.cloudfront.net/">https://d38fzyjx9jg8fj.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d366s8lxuwna4d.cloudfront.net/">https://d366s8lxuwna4d.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-northeast-1</td>
<td><a href="https://d3h58onr8hrozw.cloudfront.net/">https://d3h58onr8hrozw.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d13ljas036gz6c.cloudfront.net/">https://d13ljas036gz6c.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-northeast-2</td>
<td><a href="https://d11ouwvqqq1ads.cloudfront.net/">https://d11ouwvqqq1ads.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-southeast-1</td>
<td><a href="https://d2g7up6vqvaq2o.cloudfront.net/">https://d2g7up6vqvaq2o.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d12o1dl1h4w0xc.cloudfront.net/">https://d12o1dl1h4w0xc.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-southeast-2</td>
<td><a href="https://d2190hlw27bb8.cloudfront.net/">https://d2190hlw27bb8.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d3mgrlqzmisce5.cloudfront.net/">https://d3mgrlqzmisce5.cloudfront.net/</a></td>
</tr>
<tr>
<td>eu-central-1</td>
<td><a href="https://d1n9s7btyr4f0n.cloudfront.net/">https://d1n9s7btyr4f0n.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d3tqoc05lsydd3.cloudfront.net/">https://d3tqoc05lsydd3.cloudfront.net/</a></td>
</tr>
<tr>
<td>eu-west-2</td>
<td><a href="https://dl32tyuy2mmv6.cloudfront.net/">https://dl32tyuy2mmv6.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d2p8ibh10q5exz.cloudfront.net/">https://d2p8ibh10q5exz.cloudfront.net/</a></td>
</tr>
</tbody>
</table>

>Note

ca-central isn't included in the table because we host static contents behind the domain *.my.connect.aws.

If your business does not use SAML, and you have firewall restrictions, you can add the following entries per Region:

Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.
## Region or CloudFront Domain

<table>
<thead>
<tr>
<th>Region</th>
<th>CloudFront Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td><a href="https://d32i4gd7pg4909.cloudfront.net/">https://d32i4gd7pg4909.cloudfront.net/</a></td>
</tr>
<tr>
<td>us-west-2</td>
<td><a href="https://d18af777lco7lp.cloudfront.net/">https://d18af777lco7lp.cloudfront.net/</a></td>
</tr>
<tr>
<td>eu-west-2</td>
<td><a href="https://d16q6638mh01s7.cloudfront.net/">https://d16q6638mh01s7.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-northeast-1</td>
<td><a href="https://d2c2t8mxjhq5z1.cloudfront.net/">https://d2c2t8mxjhq5z1.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-northeast-2</td>
<td><a href="https://d9j3u8qaxidxi.cloudfront.net/">https://d9j3u8qaxidxi.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-southeast-1</td>
<td><a href="https://d3qzmd7y07pz0i.cloudfront.net/">https://d3qzmd7y07pz0i.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-southeast-2</td>
<td><a href="https://dwcpoxuuza83q.cloudfront.net/">https://dwcpoxuuza83q.cloudfront.net/</a></td>
</tr>
<tr>
<td>eu-central-1</td>
<td><a href="https://d1whcm49570jjw.cloudfront.net/">https://d1whcm49570jjw.cloudfront.net/</a></td>
</tr>
<tr>
<td>ca-central-1</td>
<td><a href="https://d2wfbyspmqjmgmog.cloudfront.net/">https://d2wfbyspmqjmgmog.cloudfront.net/</a></td>
</tr>
<tr>
<td>us-gov-east-1:</td>
<td><a href="https://s3-us-gov-east-1.amazonaws.com/">https://s3-us-gov-east-1.amazonaws.com/</a></td>
</tr>
<tr>
<td>us-gov-west-1:</td>
<td><a href="https://s3-us-gov-west-1.amazonaws.com/">https://s3-us-gov-west-1.amazonaws.com/</a></td>
</tr>
</tbody>
</table>

### NLB endpoints

The following table lists the specific endpoints for the Region the Amazon Connect instance is in. If you don’t want to use the TurnNlb-*-elb.region.amazonaws.com wildcard, you can add these endpoints to your allowlist instead.

<table>
<thead>
<tr>
<th>Region</th>
<th>Turn Domain/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-west-2</td>
<td>TurnNlb-8d79b4466d82ad0e.elb.us-west-2.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>TurnNlb-dbc4ebb71307fda2.elb.us-west-2.amazonaws.com</td>
</tr>
<tr>
<td>Region</td>
<td>Turn Domain/URL</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>us-east-1</td>
<td>TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>TurnNlb-31a7fe8a79c27929.elb.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td></td>
<td>TurnNlb-7a9b8e750cec315a.elb.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>af-south-1</td>
<td>TurnNlb-29b8f2824c2958b8.elb.af-south-1.amazonaws.com</td>
</tr>
<tr>
<td>ap-northeast-1</td>
<td>TurnNlb-3c6ddabcbeb821d8.elb.ap-northeast-1.amazonaws.com</td>
</tr>
<tr>
<td>ap-northeast-2</td>
<td>TurnNlb-a2d59ac3f246f09a.elb.ap-northeast-2.amazonaws.com</td>
</tr>
<tr>
<td>ap-southeast-1</td>
<td>TurnNlb-261982506d86d300.elb.ap-southeast-1.amazonaws.com</td>
</tr>
<tr>
<td>ap-southeast-2</td>
<td>TurnNlb-93f2de0c97c4316b.elb.ap-southeast-2.amazonaws.com</td>
</tr>
<tr>
<td>ca-central-1</td>
<td>TurnNlb-b019de6142240b9f.elb.ca-central-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-central-1</td>
<td>TurnNlb-ea5316ebe2759cbc.elb.eu-central-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-west-2</td>
<td>TurnNlb-1dc64a459ead57ea.elb.eu-west-2.amazonaws.com</td>
</tr>
<tr>
<td>us-gov-west-1</td>
<td>TurnNlb-d7c623c23f628042.elb.us-gov-west-1.amazonaws.com</td>
</tr>
</tbody>
</table>
Option 2 (not recommended): Allow IP address ranges

The second option relies on using an allowlist to define the IP addresses and ports that Amazon Connect can use. You create this allowlist using the IP addresses in the AWS ip-ranges.json file.

If the Region you are using Amazon Connect in does not appear in the AWS ip-ranges.json file, use just the Global values.

For more information about this file, see About Amazon Connect IP address ranges.

<table>
<thead>
<tr>
<th>IP-Ranges entry</th>
<th>AWS Region</th>
<th>Ports/Protocols</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON_CONNECT</td>
<td>GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allowlist)</td>
<td>3478 (UDP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>EC2</td>
<td>GLOBAL and Region where your Amazon Connect instance is located (GLOBAL only if a region-specific entry doesn’t exist)</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>CLOUDFRONT</td>
<td>Global*</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>GLOBALACCELERATOR</td>
<td>GLOBAL and Region where your Amazon</td>
<td>443 (HTTPS) and 80 (HTTP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

About Amazon Connect IP address ranges
<table>
<thead>
<tr>
<th>IP-Ranges entry</th>
<th>AWS Region</th>
<th>Ports/Protocols</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

If you're using SAML Sign-In to your Amazon Connect instance, be sure to add the Global Accelerator domain to your allowlist: *.awsglobalaccelerator.com.

*CloudFront serves static content such as images or javascript from an edge location that has the lowest latency in relation to where your agents are located. IP range allow lists for CloudFront are global and require all IP ranges associated with "service": "CLOUDFRONT" in the ip-ranges.json file.

**About Amazon Connect IP address ranges**

In the AWS ip-ranges.json file, the whole /19 IP address range is owned by Amazon Connect. All traffic to and from the /19 range comes to and from Amazon Connect.

The /19 IP address range isn't shared with other services. It's for the exclusive use to Amazon Connect globally.

In the AWS ip-ranges.json file, you can see the same range listed twice. For example:

```json
{
  "ip_prefix": "15.193.0.0/19",
  "region": "GLOBAL",
  "service": "AMAZON"
},
{
  "ip_prefix": "15.193.0.0/19",
```
AWS always publishes any IP range twice: one for the specific service, and one for "AMAZON" service. There could even be a third listing for a more specific use case within a service.

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available ip-ranges.json file. They are kept for a minimum of 30 days before they are used by the service. After 30 days, softphone traffic through the new IP address ranges increases over the subsequent two weeks. After two weeks, traffic is routed through the new ranges equivalent to all available ranges.

For more information about this file and IP address ranges in AWS, see AWS IP Address Ranges.

Stateless firewalls

If you're using a stateless firewall for both options, use the requirements described in the previous sections. Then you must add to your allowlist the ephemeral port range used by your browser, as shown in the following table.

<table>
<thead>
<tr>
<th>IP-Range entry</th>
<th>Port</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON_CONNECT</td>
<td>For a Windows environment: 49152-65535 (UDP)</td>
<td>INBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td></td>
<td>For a Linux environment: 32768 - 61000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Allow DNS resolution for softphones

If you already added Amazon Connect IP ranges to your allowlist, and you don't have any restriction on DNS name resolution, then you don't need to add TurnNlb-*.*.elb.*.region.amazonaws.com to your allowlist.
• To check whether there are restrictions on DNS name resolution, while on your network, use the `nslookup` command. For example:

```bash
nslookup TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com
```

If you can't resolve the DNS, you must add the TurnNLB endpoints listed above or `TurnNlb-*.elb.region.amazonaws.com` to your allowlist.

If you don't allow this domain, your agents will get the following error in their Contact Control Panel (CCP) when they try to answer a call:

• Failed to establish softphone connection. Try again or contact your administrator with the following: Browser unable to establish media channel with turn:TurnNlb-xxxxxxxxxxxxx.elb.region.amazonaws.com:3478?transport=udp

### Port and protocol considerations

Consider the following when implementing your network configuration changes for Amazon Connect:

• You need to allow traffic for all addresses and ranges for the Region in which you created your Amazon Connect instance.

• If you are using a proxy or firewall between the CCP and Amazon Connect, increase the SSL certificate cache timeout to cover the duration of an entire shift for your agents. Do this to avoid connectivity issues with certificate renewals during their scheduled working time. For example, if your agents are scheduled to work 8 hour shifts that include breaks, increase the interval to 8 hours plus time for breaks and lunch.

• When opening ports, Amazon EC2 and Amazon Connect require only the ports for endpoints in the same Region as your instance. CloudFront, however, serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range allowlists for CloudFront are global and require all IP ranges associated with "service": "CLOUDFRONT" in ip-ranges.json.

• Once ip-ranges.json is updated, the associated AWS service will begin using the updated IP ranges after 30 days. To avoid intermittent connectivity issues when the service begins routing traffic to the new IP ranges, be sure to add the new IP ranges to your allowlist, within 30 days from the time they were added to ip-ranges.json.
• If you are using a custom CCP with the Amazon Connect Streams API, you can create a media-less CCP that does not require opening ports for communication with Amazon Connect, but still requires ports opened for communication with Amazon EC2 and CloudFront.

Region selection considerations

Amazon Connect Region selection is contingent upon data governance requirements, use case, services available in each Region, and latency in relation to your agents, contacts, and external transfer endpoint geography.

• **Agent location/network**—CCP connectivity traverses the public WAN, so it is important that the workstation has the lowest latency and fewest hops possible, specifically to the AWS Region where your resources and Amazon Connect instance are hosted. For example, hub and spoke networks that need to make several hops to reach an edge router can add latency and reduce the quality of experience.

When you set up your instance and agents, make sure to create your instance in the Region that is geographically closest to the agents. If you need to set up an instance in a specific Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your agents' computers and your Amazon Connect instance.

• **Location of your callers**—Because calls are anchored to your Amazon Connect Region endpoint, they are subject to PSTN latency. Ideally your callers and transfer endpoints are geographically located as closely as possible to the AWS Region where your Amazon Connect instance is hosted for lowest latency.

For optimal performance, and to limit the latency for your customers when they call in to your contact center, create your Amazon Connect instance in the Region that is geographically closest to where your customers call from. You might consider creating multiple Amazon Connect instances, and providing contact information to customers for the number that is closest to where they call from.

• **External transfers**—from Amazon Connect remain anchored to your Amazon Connect Region endpoint for the duration of the call. Per-minute usage continues to accrue until the call is disconnected by the recipient of the transferred call. The call is not recorded after the agent drops or the transfer completes. The contact record data and associated call recording of a transferred call are generated after the call is terminated. Whenever possible, don't transfer calls that could be transferred back into Amazon Connect, known as circular transfers, to avoid compounding PSTN latency.
Agents using Amazon Connect remotely

Remote agents, those that use Amazon Connect from a location other than those connected to your organization's main network, may experience issues relating to their local network if they have an unstable connection, packet loss, or high latency. This is compounded if a VPN is required to access resources. Ideally, the agents are located close to the AWS Region where your AWS resources and Amazon Connect instance are hosted, and have a stable connection to the public WAN.

Rerouting audio

When rerouting audio to an existing device, consider the location of the device in relation to your Amazon Connect Region. This is so you can account for potential additional latency. If you reroute your audio, whenever there is a call intended for the agent, an outbound call is placed to the configured device. When the agent answers the device, that agent is connected with the caller. If the agent does not answer their device, they are moved into a missed contact state until they or a supervisor changes their state back to available.

Using AWS Direct Connect

Contact Control Panel (CCP) network connectivity issues are most often rooted in your route to AWS using private WAN/LAN, ISP, or both. While AWS Direct Connect does not solve issues specific to private LAN/WAN traversal to your edge router, it can help solve for latency and connectivity issues between your edge router and AWS resources. AWS Direct Connect provides a durable, consistent connection rather than relying on your ISP to dynamically route requests to AWS resources. It also allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN.

Agent workstation networking requirements for web calling voice/video

The Amazon Connect in-app, web, and video calling capabilities enable your customers to contact you without ever leaving your web or mobile application. The video calling capabilities leverage the Amazon Chime SDK communication primitives for the video stream. The voice experience is handled through Amazon Connect.
**Important**

Video calling does not support VDI environments.

The following table shows the additional networking requirements for your agents' workstation.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Subnet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.chime.aws</td>
<td>99.77.128.0/18</td>
<td>443 (TCP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3478 (UDP)</td>
</tr>
</tbody>
</table>

The following diagram shows the networking requirements for the customers who are using the communications widgets to contact you.
Detailed network paths for Amazon Connect

Voice calls

The following diagram shows how voice calls flow through Amazon Connect:

1. Users access the Amazon Connect application using a web browser. All communications are encrypted in transit using TLS.

2. Users establish voice connectivity to Amazon Connect from their browser using WebRTC. Signaling communication is encrypted in transit using TLS. Audio is encrypted in transit using SRTP.

3. Voice connectivity to traditional phones (PSTN) is established between Amazon Connect and AWS telecommunications carrier partners using private network connectivity. In cases where shared network connectivity is used, signaling communication is encrypted in transit using TLS and audio is encrypted in transit using SRTP.

4. Call recordings are stored in your Amazon S3 bucket that Amazon Connect has been given permissions to access. This data is encrypted between Amazon Connect and Amazon S3 using TLS.
5. Amazon S3 server-side encryption is used to encrypt call recordings at rest using a customer-owned KMS key.

### Authentication

The following diagram shows using the AD Connector with AWS Directory Service to connect to an existing customer Active Directory installation. The flow is similar to using AWS Managed Microsoft AD.

1. The user's web browser initiates authentication to an OAuth gateway over TLS using the public internet with user credentials (Amazon Connect login page).
2. OAuth gateway sends the authentication request over TLS to AD Connector.
3. AD Connector does LDAP authentication to Active Directory.
4. The user's web browser receives OAuth ticket back from gateway based on authentication request.
5. The client loads the Contact Control Panel (CCP). The request is over TLS and uses OAuth ticket to identify user/directory.
Using Amazon Connect in a VDI environment

Virtual Desktop Infrastructure (VDI) environments add another layer of complexity to your solution that warrants separate POC efforts and performance testing to optimize. The Amazon Connect Contact Control Panel (CCP) can operate in thick, thin, and zero client VDI environments as any other WebRTC based browser application does, and the configuration/support/optimization is best handled by your VDI support team. That being said, the following is a collection of considerations and best practices that have been helpful for our VDI-based customers.

- **Location of your agents**—Ideally, there are as few hops as possible with the lowest round trip time between the location from which your agents use the CCP and the VDI host location.

- **Host location of your VDI solution**—Ideally, your VDI host location is on the same network segment as your agents, with as few hops as possible from both internal resources as well as an edge router. You also want the lowest round-trip time possible to both WebRTC and Amazon EC2 range endpoints.

- **Network**—Each hop that traffic goes through between endpoints increases the possibility of failure and adds opportunity to introduce latency. VDI environments are particularly susceptible to call quality issues if the underlying route is not optimized or the pipe isn't either fast or wide enough. While AWS Direct Connect can improve call quality from the edge router to AWS, it will not address internal routing issues. You may need to upgrade or optimize your private LAN/WAN, or redirect to an external device to circumvent call audio issues. In most scenarios, if this is required, the CCP is not the only application that is having issues.

- **Dedicated resources**—at the Network and desktop level are recommended to prevent an impact to available agent resources from activities, such as backups and large file transfers. One way to prevent resource contention is by restricting the desktop access to Amazon Connect users who will be using their environment similarly, instead of sharing resources with other business units who may use those resources differently.

- **Using a soft phone with remote connections**—in VDI environments can cause impact to audio quality.

**Tip**

If your agents connect to a remote endpoint and operates in that environment, we recommend either rerouting audio to an external E.164 endpoint or connecting the media through the local device and then signaling through the remote connection.
You can build a custom CCP with the Amazon Connect Streams API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. For more information about the streams API, see the GitHub repository at https://github.com/aws/amazon-connect-streams.

CCP connectivity

When an agent logs in, the CCP attempts to connect to the Amazon EC2 signaling endpoints listed in the AWS ipranges.json file, Amazon Connect for media, and CloudFront for web artifacts such as images. When the agent logs out or the browser is closed, endpoints are reselected when the agent next logs in. If a connection to Amazon EC2 or Amazon Connect fails, errors display on the CCP. If a connection to CloudFront fails, web elements such as buttons and icons, or even the page itself fails to load correctly.

Outbound calls

- When an outbound call is placed, the event signal is sent to the Amazon EC2 endpoint, which then communicates with Amazon Connect to place the call. Upon a successful dial attempt, the agent is bridged in, which anchors the call to the agent's Amazon Connect endpoint. Any external transfers or conferences also uses the anchor until the call is disconnected. Anchoring can help reduce PSTN latency.

Inbound calls

- When an inbound call is received, the call is anchored to an Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- When an agent is available, the call is pushed through using a new Amazon EC2 connection to their browser and offered to the agent.
- When the agent accepts the call and either the external device has been answered or the CCP determines it can receive a call, a connection to Amazon Connect is established for call media to the agent.
Transferred calls

- When a call is transferred, the transfer event that signals to place an outbound call to the specified transfer destination is sent to Amazon EC2, which then communicates with Amazon Connect to place the call.

- When the call is connected, the agent is bridged in, anchoring the call to the agent's existing Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.

- If the agent hangs up after the call is bridged, the agent's connection to the call is terminated, but Amazon Connect hangs on to the call at the Amazon Connect anchor point until there is a far side disconnect. When the call is disconnected, contact records and associated recordings are generated and made available for the call.

Missed calls

- If the call is waiting on an agent, customer queue flow logic is used until an agent is available and the call has been successfully routed to that agent.

- If the agent does not accept the call, the agent moves into a Missed Call state and is unable to take calls until the agent, or a call center manager, changes their status to Available again. The caller does not hear ringing while the call is waiting for the agent, and continues to hold until connected with an agent as defined in the customer queue flow logic.

- If the agent is configured for cross-channel concurrency, they must clear the missed contact before any other contacts on any other channel can be routed to them. For example, if they are configured to handle voice and chats at the same time, and they miss a chat, they must clear that contact before any other voice or chat contacts are routed to them.

Panic logout

- If the browser window where the CCP is running is closed, the call remains connected, but opening the browser and logging back in will not allow you to re-establish the media connection. You are still able to transfer or end the call, but no audio path is established between the agent and caller.
Use an allowlist for integrated applications

All domains that embed the CCP for a particular instance must be explicitly allowed for cross-domain access to the instance. For example, to integrate with Salesforce, you must place your Salesforce Visualforce domain in an allowlist.

To allow a domain URL

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from Instance Alias.
3. In the navigation pane, choose Approved origins.
4. Choose Add origin.
5. Type the URL and choose Add.

Update your Amazon Connect domain

We are in the process of updating the Amazon Connect console with a new URL:

- https://your-instance-alias.my.connect.aws/

This change will occur automatically.

Note

To prepare for this change, you need to change any hardcoded or bookmarked links. If your old link looks like this:

- https://your-instance-alias.awsapps.com/connect/

Change to:

- https://your-instance-alias.my.connect.aws/

In addition, there are other steps you will need to take if you use a firewall, SAML, or other connectors such as Salesforce. This topic provides information you need to consider when migrating to the new domain.
Firewall allowlist

Add the following new domains to your allowlist:

- `your-instance-alias.my.connect.aws/ccp-v2`
- `your-instance-alias.my.connect.aws/api`
- `*.static.connect.aws`

⚠️ Important

Do not remove the domains already in your allowlist:

- `your-instance-alias.awsapps.com/connect/ccp-v2`
- `your-instance-alias.awsapps.com/connect/api`
- `*.cloudfront.net`

For more information about setting up your allowlist, see [Set up your network](#).

Transport Layer Security (TLS)

We require your TLS protocol to be TLS 1.2 and recommend TLS 1.3. The new domain does not support TLS 1.1 and TLS 1.0.

We recommend that you review the new TLS policy: [ALB FS-1-2-Res-2019-08](#). For reference, you can find the previous TLS policy here: [CloudFront TLSv1](#).
Custom code and integrations

Review and replace hard-coded references to the previous domain with the new domain. For example, if you have a custom Contact Control Panel (CCP) integration, it likely relies on embedded URLs. Following are tips for updating this type of integration.

**Active Directory**

If you use Active Directory to manage identity and have an Amazon Connect managed or customer managed instance, then update `ccpUrl` to the new domain. The next time a user accesses the CCP they will be prompted to login to the new domain (one time only).

**SAML 2.0**

If you use SAML 2.0 to manage identity, then do the following steps:

- Update `ccpUrl` in your Amazon Connect Streams to the new domain `your-instance-alias.my.connect.aws/ccp-v2`.
- When you configure the relay state for your identity provider, update the `loginUrl` with `new_domain=true`.
- You must use URL encoding for the destination and `new_domain` in the URL.

If you have old instances that were set up with SAML, do the following steps:

1. If `loginUrl` contains `destination=%2Fconnect%2Fyour-destination-endpoint`, remove the `%2Fconnect` endpoint prefix from the new domain destination.
2. Add `new_domain=true` before or after `destination=%2Fyour-destination-endpoint`. It should be separated by `&`.
3. If `loginUrl` does not contain `destination` or any other parameter, add `?new_domain=true` after the relay state URL.

Following are examples of valid relay state URLs:

Note

If the RelayState is itself a parameter to another URL, then the whole RelayState itself must be URL encoded, on top of any URL encoding previously done on the destination. For example, if the derived RelayState was https://us-east-1.console.aws.amazon.com/connect/federate/your-instance-id?destination=%2Fccp-v2%2Fchat&new_domain=true, and it needs to be inserted in https://my.idp.com/signin?RelayState=<here>, then the final URL should look like https://my.idp.com/signin?RelayState=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fconnect%2Ffederate%2Fyour-instance-id%3Fdestination%3D%252Fccp-v2%252Fchat%26new_domain%3Dtrue. The URL encoding is crucial to allow it to be parsed correctly in a query string.

Other connectors

If you use Salesforce, Zendesk, ServiceNow, or other connectors:

1. Upgrade to the latest version of your connector.
2. In your connector, go to the settings and update the Amazon Connect domain that is stored there. Follow the SAML tips if applicable.

API endpoint access

If your team uses hardcoded/bookmarked URLs to access API endpoints, remove '/connect' from those domains, and change the URL to your-instance-alias.my.connect.aws.

For example, if you are using a link that looks like this to access call recordings:

- https://your-instance-alias.awsapps.com_/connect_/get-recording

Change the link to:

- https://your-instance-alias.my.connect.aws/get-recording
Personal settings

Notify your team to the upcoming change so they can take steps to prevent confusion and disruption. If you have internal documentation that includes links, please review and update accordingly. Encourage team members to update their browser bookmarks for the login page, and productivity apps, such as Alfred.

To ensure a seamless transition for your team, we encourage you to take steps to identify any missed URL references.
Create Amazon Connect Flows

A flow defines the customer experience with your contact center from start to finish. Amazon Connect includes a set of default flows so you can quickly set up and run a contact center. However, you may want to create custom flows for your specific scenario.

Contents

• Permissions required to view, edit, create flows
• Default flows
• Sample flows
• Flow block definitions
• Create a flow
• Attach a claimed or ported phone number to a flow
• Flow modules for reusable functions
• Create prompts
• Set up contact transfers
• Set up recording behavior
• Set up queued callback by creating flows, queues, and routing profiles
• Import/export flows
• Add an Amazon Lex bot to Amazon Connect
• Invoke AWS Lambda functions
• Set up live media streaming of customer audio
• Encrypt customer input
• Track events as customers interact with flows
• Use Amazon Connect contact attributes
• Migrate flows to a different instance

Permissions required to view, edit, create flows

To view, edit, create, and publish flows you need Flows permissions added to your security profile.
By default users who are assigned to the **Admin** and **CallCenterManager** security profiles have Flows permissions.

### Default flows

Amazon Connect includes a set of default flows that have already been published. It uses them to power your contact center.

For example, say you create a flow that includes putting the customer on hold, but you don't create a prompt for it. The default flow, **Default agent hold**, will be played automatically. This is a way to help you get started with your call center quickly.

#### Tip

If you want to change the behavior of a default flow, we recommend creating a new customized flow based on the default. Then call the new flow intentionally in your flows rather than defaulting to it. This gives you better control over how your flows work.

To see the list of default flows in the Amazon Connect console, go to **Routing, Flows**. They all start with **Default** in their name.

**Contents**

- Change a default flow
- **Default agent hold**: "You are on hold"
- **Default agent transfer**: "Transferring now"
- **Default customer queue**: queue hold message and music
- **Default customer whisper**: beep sound
- **Default agent whisper**: name of the queue
- **Set the default whisper flow for a chat conversation**
- **Default customer hold**: hold music
- **Default outbound**: "This call is not being recorded"
- **Default queue transfer**: "Now transferring"
- **Default prompts from Amazon Lex**: "Sorry .. "

---

**Default flows**
Change a default flow

You can override the way the default flows work by editing them directly.

Generally we recommend creating new flows based on the defaults, rather than editing the default flow directly. You can make a copy of the default flow, assign a name that indicates it's a custom version, and then edit that one. This gives you more control over how your flows work.

Change how a default flow works

The following steps show how to change the default message customers hear when they are put in a queue to wait for the next available agent.


2. Choose the default flow you want to customize. For example, choose Default customer queue if you want to create your own message when a customer is put in queue instead of using the one we've provided. This is shown in the following image.

![Contact flows table]

3. To customize the message, choose the Loop prompts block to open the properties page.
4. On the *Properties* page of the *Loop prompts* block, use the dropdown box to either choose different music, or set to *Text to Speech*. Type a message to be played.

For example, the following image shows the message "*Thank you for calling. Did you know you can reset your own password at the login page? Choose Reset now, and following the prompts.*"
5. Choose **Save** at the bottom of the properties page.

6. Choose **Publish**. Amazon Connect starts playing the new message almost immediately (it may take a few moments for it to fully take effect).
Copy a default flow before customizing it

Use the following steps to create a new flow based a current default.

2. Choose the default flow you want to customize.
3. In the upper right corner of the page, choose the Save drop-down arrow. Choose Save as, as shown in the following image.
4. Assign a new name for the flow, for example, Customer hold message.
5. Add the new flow (in this case, **Customer hold message**) to the flows you create so it's run instead of the default.

**Default agent hold: "You are on hold"

The **Default agent hold** flow is the experience the agent receives when placed on hold. During this flow, a **Loop prompt** block plays the message "You are on hold" to the agent every 10 seconds.
You can set **break time** to a maximum of 10 seconds. This means the maximum amount time you can specify between **You are on hold** messages is 10 seconds. To make the time between longer, add multiple prompts to the loop. For example, if you want 20 seconds between **You are on hold** messages:

- The first prompt may say **You are on hold** with **break time="10s"**
- Add another prompt with a blank message and **break time="10s"**.

For instructions about how to override and change a default flow, see [Change a default flow](#).
Tip

Wondering if a default flow has been changed? Use flow version control to view the original version of the flow.

Default agent transfer: "Transferring now"

This default transfer flow is what the "from" agent experiences when they transfer a contact to another agent by using Create quick connects. The "from" agent hears a Play prompt play the message "Transferring now." Then the Transfer to agent block is used to transfer the contact to the agent.

When the contact is transferred, the "to" agent hears the Default agent whisper.

Tip

The Transfer to Agent block is a beta feature and only works for voice interactions. To transfer a chat contact to another agent, follow these instructions: Use contact attributes to route contacts to a specific agent.

For instructions about how to override and change a default flow, see Change a default flow.

Tip

Wondering if a default flow has been changed? Use flow version control to view the original version of the flow.

Default customer queue: queue hold message and music

This default flow is played when a customer is placed in a queue.

1. The loop has a one-time voice prompt:

   Thank you for calling. Your call is very important to us and will be answered in the order it was received.
2. It plays queue music in .wav format that's been uploaded to the Amazon Connect instance.

3. The customer remains in this loop until their call is answered by an agent.

**Change the default message a customer hears when they are put in queue**

The following steps show how to change the default message customers hear when they are put in a queue to wait for the next available agent.

1. On the navigation menu, choose **Routing, Flows**.

2. On the **Flows** page, choose **Default customer queue**, as shown in the following image.

3. To customize the message, choose the **Loop prompts** block to open the properties page.
4. Use the dropdown box to either choose different music, or set to **Text to Speech** and then type a message to be played,

For example, the following image shows the message "Thank you for calling. Did you know you can reset your own password at the login page? Choose Reset now, and following the prompts."

5. Choose **Save** at the bottom of the properties page.

6. Choose **Publish**. Amazon Connect starts playing the new message almost immediately (it may take a few moments for it to fully take effect).
Default customer whisper: beep sound

This flow uses a Set whisper flow block to play a message for the customer when the customer and agent are joined. It uses a "beep" sound to notify a customer that their call has been connected to an agent.

Use the Set whisper flow block to override the default agent whisper in a voice conversation.

⚠️ Important

For chat conversations, you need to include a Set whisper flow for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation.

Default agent whisper: name of the queue

This flow uses a Set whisper flow block to play a message for the agent when the customer and agent are joined.

The name of the queue is played to the agent. It identifies the queue that the customer was in. The name of the queue is retrieved from the system variable $.Queue.Name.

Use the Set whisper flow block to override the default agent whisper in a voice conversation.
Important
For chat conversations, you need to include a Set whisper flow for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation.

For more information about system variables, see System attributes.

Tip
Wondering if a default flow has been changed? Use flow version control to view the original version of the flow.

Set the default whisper flow for a chat conversation

For chat conversations, you need to include a Set whisper flow block for default agent or customer whispers to play.

For example, to set the default whisper flow for chats that use the Sample inbound flow:

1. Go to Routing, Flows, and choose the Sample inbound flow.
2. Add a Set whisper flow block after the chat channel has branched, as shown in the following image:
3. In the **Set whisper flow** block, open the properties page, and choose the flow you want to play as the default for chat conversations. For example, you might choose **Default whisper flow** to show agents the name of the originating queue in the chat window. This is helpful when agents are managing more than one queue.

![Set whisper flow block](image)

4. Choose **Save**.

**Default customer hold: hold music**

This flow starts when the customer is put on hold. It plays the audio that the customer hears while on hold.

For instructions about how to override and change a default flow, see [Change a default flow](#).

**Tip**

Wondering if a default flow has been changed? Use [flow version control](#) to view the original version of the flow.
Default outbound: "This call is not being recorded"

This flow is an outbound whisper that manages what the customer experiences as part of an outbound call, before being connected with an agent.

1. It starts with an optional **Set recording behavior** block. Then a prompt plays the following message:

   *This call is not being recorded.*

2. The flow ends.

3. The customer remains in the system (on the call) after the flows ends.

For instructions about how to override and change a default flow, see [Change a default flow](#).

**Tip**

Wondering if a default flow has been changed? Use [flow version control](#) to view the original version of the flow.

Default queue transfer: "Now transferring"

This flow manages what the agent experiences when they transfer a customer to another queue.

It starts with a **Check hours of operation** block to check the hours of operation for the current queue. The **In hours** option branches to the **Check staffing** block to determine whether agents are available, staffed, or online.

If it returns **True** (agents are available), the flow goes to the **Transfer to queue** block. If it returns **False** (no agents are available), the flow plays a prompt and disconnects the call.

For instructions about how to override and change a default flow, see [Change a default flow](#).

**Tip**

Wondering if a default flow has been changed? Use [flow version control](#) to view the original version of the flow.
Default prompts from Amazon Lex: "Sorry .. "

If you add an Amazon Lex classic bot (not Amazon Lex V2) to your contact center, know that it also has some default prompts that it uses for error handling. For example:

- Sorry, can you please repeat that?
- Sorry, I could not understand. Goodbye.

To change default Amazon Lex prompts

1. In Amazon Lex, go to your bot.
2. On the Editor tab, choose Error Handling.
3. Change the text as needed. Choose Save, then Build and Publish.

Sample flows

Amazon Connect includes a set of sample flows that show you how to perform common functions. They are designed to help you learn how to create your own flows that work in a similar way. For example, if you want to add a queued callback flow to your call center, take a look at the Sample queued callback flow.

To explore how the sample flows work

1. Claim a number if you haven't already: go to Channels, Phone numbers, Claim a number.
2. Choose the DID tab, then choose a number.
3. In Flow / IVR use the drop down to choose the sample flow you want to try. Click Save.
4. Call the number. The sample flow that you selected starts.

   We recommend opening the sample flow in the flow designer and following along to see how it works while you're experiencing it.

To open a sample flow in the flow designer

1. In Amazon Connect choose Routing, Flows.
2. On the Flows page, scroll down to the flows with names that start with Sample.
3. Choose the flow you want to view.
The topics in this section describe how each of the sample flows work.

Contents

- Sample inbound flow (first contact experience)
- Sample AB test
- Sample customer queue priority
- Sample disconnect flow
- Sample queue configurations
- Sample queue customer
- Sample queued callback
- Sample interruptible queue flow with callback
- Sample Lambda integration
- Sample recording behavior
- Sample note for screenpop
- Sample secure input with agent
- Sample secure input with no agent

Sample inbound flow (first contact experience)

⚠️ Note

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)

This sample flow is automatically assigned to the phone number that you claimed when you first set up flows. For more information, see Get started.

It uses the Check contact attributes block to determine if the contact is contacting you by phone or chat, or if it is a task, and to route them accordingly.

- If the channel is chat or task, the contact is transferred to the Sample queue configurations.
• If the channel is voice, then based on user input the contact is either transferred to the other sample flows or a sample follow-up agent task is created for this contact.

The following image shows the sample inbound flow. We recommend viewing the flow in the flow designer so you can see the details.

Sample AB test

Note

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)

This flow shows how to perform an A/B call distribution based on a percentage. Here's how it works:

1. The Play prompt block uses Amazon Polly, the text-to-speech service, to say "Amazon Connect will now simulate rolling dice by using the Distribute randomly block. Now rolling."
2. The contact reaches the **Distribute by percentage** block, which routes the customer randomly based on a percentage.

   **Distribute by percentage** simulates a dice roll, resulting in a values between 2 to 12 with different percentages. For example, there is 3 percent chance for the "2" option, 6 percent chance for the "3" option, and so on.

3. After the contact gets routed, the **Play prompt** tells the customer which number the dice rolled.

4. At the end of the sample, the **Transfer to flow** block transfers the customer back to the [Sample inbound flow](#).

### Sample customer queue priority

**Note**

This sample flow is available in previous Amazon Connect instances. In new instances, you can see this functionality in [Sample queue configurations](#).

Type: Flow (inbound)

By default the priority for new contacts is 5. Lower values raise the priority of the contact. For example, a contact assigned a priority of 1 is routed first.

This sample shows how you can use the **Change routing priority/age block** to raise or lower the priority of a contact in a queue. Using this block, there are two ways you can raise or lower a customer’s priority:

- Assign them a new priority value, such as 1, to raise their priority.
- Or, increase the routing age of the contact. Customers who are queued longer are routed first, when all contacts have the same queue priority value (such as 5).

### Option 1: Raise the priority

- The **Get Customer Input** block prompts the customer to press 1 to move to the front of the queue. This block gets the customer's input; it doesn't actually change the customer's priority.
• If the customer presses 1, they go down the "Pressed 1" branch, which takes them to the **Change routing priority/age block**. This block changes their priority in the queue to 1, which is the highest priority.

**Option 2: Change the routing age**

• The **Get Customer Input** block prompts the customer to press 2 to move behind existing contacts already in queue. This block gets the customer's input; it doesn't actually change the customer's priority.

• If the customer presses 2, they go down the "Pressed 2" branch, which takes them to a different **Change routing priority/age** block. This block increases their routing age by 10 minutes. This has the effect of moving them ahead of others in the queue who have been waiting longer.

**Sample disconnect flow**

!!! **Note**

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see [Sample flows](#).

Type: Flow (inbound)

This sample works with voice, chat, and task contacts.

**Chat contacts**

1. The **Play prompt** block shows a text message that the agent has disconnected.
2. A **Wait** block sets the timeout period for 15 minutes. If the customer returns in 15 minutes, the customer is transferred to a queue to chat with another agent.
3. If the customer doesn't return, the timer expires and the chat disconnects.

**Voice contacts**

1. Sets a user-defined attribute, DisconnectFlowRun. If it = Y, disconnect.
2. Gets customer input, whether they were happy with service.
3. Terminates flow.

**Task contacts**

1. Checks contact attributes, whether Agent ARN = NULL.
2. Transfers to agent's queue.
3. If at capacity, disconnects.

For a list and description of all the disconnect reasons, see `DisconnectReason` in the `ContactTraceRecord`.

**Sample queue configurations**

*Note*

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)

This flow shows different ways you can put a customer in queue: you can change the priority of the customer, determine the wait time in queue, and give them an option for a callback. Here's how it works:

1. The customer is put in the BasicQueue.
2. After that, the **Default customer queue** flow is invoked. This block runs a **Loop prompts** block that plays the following:

   *Thank you for calling. Your call is very important to us and will be answered in the order it was received.*

3. The hours of operation are checked with a **Check hours of operation** block.
4. The channel is checked with a **Check contact attributes** block:

   - If chat, we check the time in queue. If it's less than 5 minutes, the customer is placed in queue for an agent. If it's more, we check the channel again and if it's chat, put the customer in queue for an agent.
• If voice, the customer is routed down the **No Match** branch, to a **Play prompt** block and then to a **Get customer input** block.

In the **Get customer input** block, we give the customer the option to press 1 to move to the front of the queue or 2 to move to the end of the queue.

The two **Change routing priority / age** blocks move the customer to the front or back of the queue.

The following image of the sample flow shows this page highlighted:

5. Next we use a **Check queue status** block to check whether the time in queue is less than 300 seconds.
6. We use a **Play prompt** block to tell the customer the results.
7. We use a **Check contact attributes** block again to check the customer's channel: chat or voice/No Match.

These next steps apply to customers who were routed down the voice/No Match branch, as shown in the following image:
1. In the **Get customer input** block, we prompt customers to *Press 1 to go into queue or 2 to enter a callback number.*

2. If customers press 2, they are routed down the **Pressed 2** branch to the **Store customer input** block.

3. The **Store customer input** block prompts the customer for their phone number.

4. The customer's phone number is stored in the **Stored customer input attribute**, by the **Set callback number** block.

5. We use a **Transfer to queue** block to put the customer in a callback queue.

6. The **Transfer to queue** block is configured so Amazon Connect waits 5 seconds between the time the callback contact is initiated and the contact is enqueued, where it sits until it is offered to an available agent.

   If the initial callback doesn't reach the customer, Amazon Connect will attempt 1 callback. If it were configured for 2 attempted callbacks, it would wait 10 minutes between each one.

   Also, no special callback queue is specified. Rather, customers are in the BasicQueue, which was set at the beginning of the flow.
For information about queued callbacks, see the following topics:

- Set up queued callback by creating flows, queues, and routing profiles
- Flow block: Transfer to queue
- About queued callbacks in metrics

Sample queue customer

Note
This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.
This flow performs checks before placing customer into a queue. Here's how it works:

1. The **Set working queue** block determines which queue to transfer the customer to.
2. The **Check hours of operation** block perform checks to avoid the customer being queued during non-working hours.
3. The customer is transferred to the queue if it is within business hours, and the queue can handle this call. Otherwise, the customer is played a message "We are not able to take your call right now. Goodbye." And then the customer is disconnected.

**Sample queued callback**

Note

This sample flow is available in previous Amazon Connect instances. In new instances, you can see examples of queued callback in [Sample interruptible queue flow with callback](#) and [Sample queue configurations](#).

Type: Flow (inbound)

This flow provides callback queue logic. Here's how it works:

1. After a voice prompt, a working queue is selected and its queue status is checked.
2. A voice prompt tells the customer if the wait time for the selected queue is longer than 5 minutes. Customers are offered a choice to wait in the queue or to be placed into a callback queue.
3. If the customer decides to wait in the queue, the **Set customer queue flow** block places them in a queue flow that provides a callback option. That is, it places them in [Sample interruptible queue flow with callback](#).
4. If the customer chooses to be placed into a callback queue, their number is stored in the **Store customer input** block. Then their callback number is set, and they are transferred to the callback queue.

For information about queued callbacks, see the following topics:

- [Set up queued callback by creating flows, queues, and routing profiles](#)
Sample interruptible queue flow with callback

Note
This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Customer queue

This flow shows you how to manage what the customer experiences while in queue. It uses Check contact attributes to determine if the customer is contacting you by phone or chat, and to route them accordingly.

If the channel is chat, the customer is transferred to the Loop prompts.

If the channel is voice, the customer hears a looping audio that interrupts every 30 seconds to give them two options from the Get customer input block:

1. The customer can press 1 to enter a callback number. Then the Get customer input block prompts the customer for their phone number. Then the flow ends.
2. Press 2 ends the flow, and the customer remains in the queue.

Sample Lambda integration

Note
This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)
This flow shows you how to invoke a Lambda function and do a data dip, that is, retrieve information about the customer. The data dip uses the caller's phone number to look up the US state they are calling from. If the customer is using chat, it returns a fun fact. Here's how it works:

1. A prompt tells the customer that a data dip is being performed.
2. The Invoke Lambda function block triggers sampleLambdaFlowFunction. This sample Lambda function determines the location of the phone number. The function times out in 4 seconds. If it times out, it plays a prompt that says "Sorry, we failed to find the state for your phone number's area code."
3. In the first Check contact attributes block, it checks the channel the customer is using: voice, chat, task. If chat, it returns a fun fact.
4. If voice, the second Check contact attributes block is triggered. It checks the match conditions of State, which is an external attribute. It uses an external contact attribute because it's getting data by using a process that's external to Amazon Connect
5. A prompt tells you that it's returning you back to Sample inbound flow, and then starts the Transfer flow block.
6. If the transfer fails, it plays a prompt and then disconnects the contact.

For more information about using attributes, see Lambda functions and attributes.

**Sample recording behavior**

⚠️ **Note**

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)

This flow starts by checking the channel of the contact:

- If the contact is a task, it is transferred to the Sample inbound flow.
- If the customer is using chat, they get a prompt that the Set recording block enables managers to monitor chat conversations. (To record chats, you only need to specify an Amazon S3 bucket where the conversation will be stored.)
To monitor chats, the **Set recording block** is configured to record both the **Agent and Customer**.

- If the contact is using voice, a **Get customer input** block prompts them to enter the number for who they want to record. Their entry triggers the **Set recording behavior** block with the appropriate configuration.

It ends with the customer being transferred by to the **Sample inbound flow**.

For more information, see the following topics:

- **Set up recording behavior**
- **Set up live monitoring for voice and/or chat**
- **Review recorded conversations between agents and customers using Amazon Connect**

## Sample note for screenpop

**Note**

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see **Sample flows**.

Type: Flow (inbound)

This flow shows you how to use Screenpop, a Contact Control Panel feature, to load a web page with parameters based on attributes.

In this sample flow, a **Set contact attributes** block is used to create an attribute from a text string. As an attribute, the text can be passed to the CCP to display a note to an agent.

## Sample secure input with agent

**Note**

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see **Sample flows**.
Type: Queue transfer

This flow shows you how to allow customers to input sensitive data while putting the agent on hold. In a production environment, we recommend using encryption instead of this solution.

Here's how it works:

1. This flow begins with checking the customer's channel. If they are using chat, they are put in a queue.
2. If they are using voice, the agent and customer are put in a conference call.
3. A Play prompt tells the customer that the agent will be put on hold while customer enters their credit card information.
4. When the prompt is finished playing, the agent is put on hold using a Hold customer or agent block. If an error occurs, a prompt is played that agent was unable to put on hold, after which the contact flow is ended.
5. The customer's input is stored using the Store Customer Input block. This block encrypts the sensitive customer information using a signing key that must be uploaded in .pem format. For a detailed walkthrough that explains how to encrypt customer input, see Creating a secure IVR solution with Amazon Connect.
6. After the customer's data is collected, the agent and customer are put back on call using the Conference All option in another Hold customer or agent block.
7. The error branch runs if there's an error while capturing the customer's data.

Sample secure input with no agent

Note

This topic explains a sample flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample flows.

Type: Flow (inbound)

This flow shows you how to capture sensitive customer data and encrypt it using a key. Here's how it works:
1. It begins by checking the contact's channel. If they are using chat, a prompt is played that this doesn't work with chat, and they are transferred to Sample inbound flow.

2. If they are using voice, the Store customer input block prompts them to enter their credit card number. The block stores and also encrypts the data using a signing key that must be uploaded in a .pem format.

   In the Set contact attributes block, the encrypted card number is set as contact attribute.

3. After the card number is successfully set as contact attribute, the customer is transferred back to the Sample inbound flow.

Flow block definitions

Use flow blocks to create flows in the flow designer. Drag flow blocks and drop them onto a canvas to arrange a flow.

The following table lists all available flow blocks that you can use. Choose any block name in the Block column for more information.

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Q in Connect</td>
<td>Associates an Amazon Q in Connect domain to a contact to enable real-time recommendations.</td>
</tr>
<tr>
<td>Call phone number</td>
<td>Initiates an outbound call from an outbound whisper flow.</td>
</tr>
<tr>
<td>Cases</td>
<td>Gets, updates, and creates cases.</td>
</tr>
<tr>
<td>Change routing priority / age</td>
<td>Changes the priority of the contact in queue. You may want to do this, for example, based on the contact's issue or other variable.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Check call progress</strong></td>
<td>Engages with the output provided by an answering machine, and provides branches to route the contact accordingly. This block works with outbound campaigns only.</td>
</tr>
<tr>
<td><strong>Check contact attributes</strong></td>
<td>Checks the values of contact attributes.</td>
</tr>
<tr>
<td><strong>Check hours of operation</strong></td>
<td>Checks whether the contact is occurring within or outside of the hours of operation defined for the queue.</td>
</tr>
<tr>
<td><strong>Check queue status</strong></td>
<td>Checks the status of the queue based on specified conditions.</td>
</tr>
<tr>
<td><strong>Check Voice ID</strong></td>
<td>Branches based on the enrollment status, voice authentication status, or status of detection of fraudsters in a watchlist of the caller returned by Voice ID.</td>
</tr>
<tr>
<td><strong>Check staffing</strong></td>
<td>Checks the current working queue, or queue you specify in the block, for whether agents are available, staffed, or online. Staffed availability could be on call, or after contact work status.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Create persistent contact association</strong></td>
<td>Specify an attribute to create a persistent contact association, enabling conversations to continue from where they left off.</td>
</tr>
<tr>
<td><strong>Create task</strong></td>
<td>Creates a new task, sets the tasks attributes, and initiates a contact flow to start the task. To learn more about Amazon Connect Tasks, see Concepts: Tasks in Amazon Connect.</td>
</tr>
<tr>
<td><strong>Customer profiles</strong></td>
<td>Enables you to retrieve, create, and update a customer profile.</td>
</tr>
<tr>
<td><strong>Disconnect / hang up</strong></td>
<td>Disconnects a contact.</td>
</tr>
<tr>
<td><strong>Distribute by percentage</strong></td>
<td>Routes customers randomly based on a percentage.</td>
</tr>
<tr>
<td><strong>End flow / Resume</strong></td>
<td>Ends the current flow without disconnecting the contact.</td>
</tr>
<tr>
<td><strong>Get customer input</strong></td>
<td>Branches based on customer intent.</td>
</tr>
<tr>
<td><strong>Get queue metrics</strong></td>
<td>Retrieves real-time metrics about queues and agents in your contact center and returns them as attributes.</td>
</tr>
<tr>
<td><strong>Hold customer or agent</strong></td>
<td>Places a customer or agent on or off hold.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Invoke AWS Lambda function</strong></td>
<td>Calls AWS Lambda, optionally returns key-value pairs.</td>
</tr>
<tr>
<td><strong>Invoke module</strong></td>
<td>Calls a published module.</td>
</tr>
<tr>
<td><strong>Loop</strong></td>
<td>Loops through, or repeats, the <strong>Looping</strong> branch for the number of loops specified.</td>
</tr>
<tr>
<td><strong>Loop prompts</strong></td>
<td>Loops a sequence of prompts while a customer or agent is on hold or in queue.</td>
</tr>
<tr>
<td><strong>Play prompt</strong></td>
<td>Plays an interruptible audio prompt, delivers a text-to-speech message, or delivers a chat response.</td>
</tr>
<tr>
<td><strong>Set callback number</strong></td>
<td>Sets a callback number.</td>
</tr>
<tr>
<td><strong>Set contact attributes</strong></td>
<td>Stores key-value pairs as contact attributes.</td>
</tr>
<tr>
<td><strong>Customize the name of a block</strong></td>
<td>Allows you to specify custom names for your flow blocks.</td>
</tr>
<tr>
<td><strong>Set customer queue flow</strong></td>
<td>Specifies the flow to invoke when a customer is transferred to a queue.</td>
</tr>
<tr>
<td><strong>Set disconnect flow</strong></td>
<td>Sets the flow to run after a disconnect event.</td>
</tr>
<tr>
<td><strong>Set event flow</strong></td>
<td>Specifies which flow to run during a contact event.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Set hold flow</strong></td>
<td>Links from one flow type to another.</td>
</tr>
<tr>
<td><strong>Set logging behavior</strong></td>
<td>Enables flow logs so you can track events as contacts interact with flows.</td>
</tr>
<tr>
<td><strong>Set Voice ID</strong></td>
<td>Sends audio to Amazon Connect Voice ID to verify the caller's identity and match against fraudsters in watchlist, as soon as the call is connected to a flow.</td>
</tr>
<tr>
<td><strong>Set recording and analytics behavior</strong></td>
<td>Sets options for recording conversations.</td>
</tr>
<tr>
<td><strong>Set voice</strong></td>
<td>Sets the text-to-speech (TTS) language and voice to be used in the flow.</td>
</tr>
<tr>
<td><strong>Set whisper flow</strong></td>
<td>Overrides the default whisper by linking to a whisper flow.</td>
</tr>
<tr>
<td><strong>Set working queue</strong></td>
<td>Specifies the queue to be used when Transfer to queue is invoked.</td>
</tr>
<tr>
<td><strong>Show view</strong></td>
<td>Configures UI based workflows that you can surface to users in front end applications.</td>
</tr>
<tr>
<td><strong>Start media streaming</strong></td>
<td>Starts capturing customer audio for a contact.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Stop media streaming</strong></td>
<td>Stops capturing customer audio after it is started with a <a href="#">Start media streaming</a> block.</td>
</tr>
<tr>
<td><strong>Store customer input</strong></td>
<td>Stores numerical input to a contact attribute.</td>
</tr>
<tr>
<td><strong>Transfer to agent (beta)</strong></td>
<td>Transfers the customer to an agent.</td>
</tr>
<tr>
<td><strong>Transfer to flow</strong></td>
<td>Transfers the customer to another flow.</td>
</tr>
<tr>
<td><strong>Transfer to phone number</strong></td>
<td>Transfers the customer to a phone number external to your instance.</td>
</tr>
<tr>
<td><strong>Transfer to queue</strong></td>
<td>In most flows, this block ends the current flow and places the customer in queue. When used in a customer queue flow, this block transfers a contact already in a queue to another queue.</td>
</tr>
<tr>
<td><strong>Wait</strong></td>
<td>Pauses the flow.</td>
</tr>
</tbody>
</table>

**Supported channels for flow blocks**

The following table lists all available flow blocks, and whether they support routing a contact through the specified channels.

<table>
<thead>
<tr>
<th>Block</th>
<th>Voice</th>
<th>Chat</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Q in Connect</td>
<td>Yes</td>
<td>Yes</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Block</td>
<td>Voice</td>
<td>Chat</td>
<td>Task</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Call phone number</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Cases</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Change routing priority / age</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Check call progress</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Check contact attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Check hours of operation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create persistent contact association</td>
<td>No - Error branch</td>
<td>Yes</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Check queue status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Check Voice ID</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Check staffing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create task</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Customer profiles</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Disconnect / hang up</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribute by percentage</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End flow / Resume</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Block</td>
<td>Voice</td>
<td>Chat</td>
<td>Task</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------</td>
<td>--------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Get customer input</td>
<td>Yes</td>
<td>Yes when Amazon Lex is used</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Otherwise, No - Error branch</td>
<td></td>
</tr>
<tr>
<td>Get queue metrics</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hold customer or agent</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Invoke AWS Lambda function</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Invoke module</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Loop</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Loop prompts</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Play prompt</td>
<td>Yes</td>
<td>Yes</td>
<td>No - takes the Okay branch, but it has no effect</td>
</tr>
<tr>
<td>Set callback number</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Set contact attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set customer queue flow</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set disconnect flow</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set hold flow</td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Set logging behavior</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set recording and analytics behavior</td>
<td>Yes</td>
<td>Yes</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Block</td>
<td>Voice</td>
<td>Chat</td>
<td>Task</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Set Voice ID</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Set voice</strong></td>
<td>Yes</td>
<td>No - Success branch</td>
<td>No - Success branch</td>
</tr>
<tr>
<td><strong>Set whisper flow</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Set working queue</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Show view</strong></td>
<td>No - Error branch</td>
<td>Yes</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Start media streaming</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Stop media streaming</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Store customer input</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Transfer to agent (beta)</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Transfer to flow</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Transfer to phone number</strong></td>
<td>Yes</td>
<td>No - Error branch</td>
<td>No - Error branch</td>
</tr>
<tr>
<td><strong>Transfer to queue</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Wait</strong></td>
<td>No - Error branch</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow block: Amazon Q in Connect**

**Description**

- Associates an Amazon Q in Connect domain to a contact to enable real-time recommendations.
- For more information about enabling Amazon Q in Connect, see [Use Amazon Q in Connect for generative AI–powered agent assistance in real-time](#).
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>No</td>
</tr>
</tbody>
</table>

Note

Nothing happens if a task is sent to this block, however, you will be charged. To prevent this, add a Check contact attributes block before this one and route tasks accordingly. For instructions, see Route based on contact’s channel.

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Outbound whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Amazon Q in Connect block. It specifies the full Amazon Resource Name (ARN) of the Amazon Q in Connect domain to associate to the contact.
Associate an Amazon Q Connect domain to the current contact. Amazon Q Connect recommends solutions to resolve customer issues. This block, along with Contact Lens Real-Time analytics, is used to recommend content that is related to customer issues detected during the current contact. The Set recording and analytics behavior block with Contact Lens real-time enabled must also be set in this flow for Amazon Q Connect recommendations to work. Learn more

Select a domain

Associate an Amazon Q Connect domain to this contact that will be passed through the flow as part of ContactData

- Set manually

```
arn:aws:qconnect:us-west-2:272143328558:assistant/dd02e2d4-2508-4e89-a60b-269c25498047
```
Configuration tips

- To use Amazon Q in Connect with calls, you must enable Amazon Connect Contact Lens in the flow by adding a Set recording and analytics behavior block that is configured for Contact Lens real-time. It doesn't matter where in the flow you add the Set recording and analytics behavior block.

Amazon Q in Connect, along with Contact Lens real-time analytics, is used to recommend content that is related to customer issues detected during the current call.

- Contact Lens is not required to use Amazon Q in Connect with chats.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.

![Configured block](image)

Flow block: Call phone number

Description

- Use to place an outbound call from an Outbound Whisper flow.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Outbound Whisper flow

Properties

The following image shows an example of what the Call phone number properties page looks like when you select a phone number manually. The Select a number from your instance option is selected, and the dropdown menu displays a list of available phone numbers claimed for your instance.
The following image shows an example of what the Call phone number properties page looks like when you select a phone number dynamically. The Use Attribute option is selected. The Namespace box is set to User-defined. The Attribute box is set to MainPhoneNumber.

Outbound whisper flows run in Amazon Connect immediately after an agent accepts the call during direct dial and callback scenarios. When the flow runs:

- The caller ID number is set if one is specified in the Call phone number block.
- If no caller ID is specified in the Call phone number block, the caller ID number defined for the queue is used when the call is placed.
- When there is an error with a call that is initiated by the Call phone number block, the call is disconnected and the agent is placed in AfterContactWork (ACW).

Only published flows can be selected as the outbound whisper flow for a queue.

⚠️ Note
To use a custom caller ID, you must open an AWS Support ticket to enable this feature. For more information, see Set up outbound caller ID.
Configured block

The following image shows an example of what this block looks like when it is configured. It shows the **Caller ID** phone number, and a **Success** branch.

![Configured block example](image)

There is no error branch for the block. If a call is not successfully initiated, the flow ends and the agent is placed in an **AfterContactWork (ACW)**.

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- [Sample customer queue priority](#)
- [Sample queue configurations](#)

Scenarios

See these topics for more information about caller ID works:

- [Set up outbound caller ID](#)

Flow block: Cases

**Tip**

Be sure to enable Amazon Connect Cases before using this block. Otherwise, you can't configure its properties.

**Description**

- Gets, updates, and creates cases.
• You can link a contact to a case, and then the contact will be recorded in the **Activity feed** of the case. When the agent accepts a contact that is linked to a case, the case automatically opens as a new tab in the agent application.

• While you can link contacts to multiple cases, there is a limit of five new case tabs automatically opening in the agent application. These will be the five most recently updated cases.

• For more information about cases, see [Amazon Connect Cases](#).

**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following **flow types**:

• All flows

**Properties: Get case**

ℹ️ **Tip**

The following screenshots refer to the legacy flow designer.

When configuring properties to get a case:

• You must provide at least one search criteria. Otherwise this block will take the **Error** branch.

  You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in [How to persist fields throughout the flow](#).
• To get cases for a given customer, add a **Customer profiles** block to the flow before creating the case. The following image shows the flow designer with a **Customer profiles** block linked from the Success branch to a **Cases** block.

Configure the **Customer profiles** block to get the customer profile. The following image shows an example of the **Customer profiles** properties page when it is configured. The **Action** box is set to **Get profile**. The **Select a search key** box is set to **Email address**. The **Use attribute** option is selected. The **Type** box is set to **Customer**. The **Attribute** box is set to **Email address**. The **Response fields** are set to **First name**, **Last name**.

![Customer profiles block configuration](image-url)
In the Cases block, on the Properties page configure the Customer ID section as shown in the following image. The Link contact to case option is set to Yes. The Request fields box is set to Customer Id. In the Customer Id section, the Use attribute option is selected. The Type box is set to Customer. The Attribute box is set to Profile ARN.

- You can specify to get only the last updated case for any search criteria. This can be achieved by selecting Get last updated case.

- You can persist case fields in the case namespace to make use of them in blocks that are in your flow after the Cases block that is configured to Get case. This can be achieved by making use of the Response fields section and selecting fields that you want to use in the other blocks.

You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in How to persist fields throughout the flow.

- The Get case properties show the options for the single-select field type.
- The Get case properties use the Contains function for text field type.
- The Get case properties use the EqualTo function for fields of type: number, boolean.
- The Get case properties use greater than or equal to for any date field search.

Contacts can be routed down the following branches:
- **Success**: The case was found.
• **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. It might be that the contact was not linked after the case is retrieved (partial success/partial failure). If this happens, then the flow will follow this branch.

• **Multiple found**: Multiple cases are found with the search criteria.

• **None found**: No cases are found with the search criteria.

• **Error**: An error was encountered while trying to find the case. This may be due to a system error or how Get case is configured.

The following images show an example of a Cases Properties page that is configured for the Get case action.

The first image shows the Properties page configured to search for a case by Customer Id and Title. The Customer Id is being pulled in from the Profile ARN of the customer. In this image, the Link contact to case option is set to Yes. The Request field is set to Customer Id, Title. In the Customer Id section, the Use attribute option is selected. The Type box is set to Customer. The Attribute box is set to Profile ARN.

This next image shows the block configured to search by Late Arrival. Under Title, the Set manually option is set to Late Arrival. The Get last updated cases option is selected. The Response field option shows the three fields that will be shown to the agent: Status, Summary, and Title.
Properties: Update case

When configuring properties to update a case:

- Add a **Get case** block before an **Update case**, as shown in the following image. Use the **Get case** block to find the case you want to update.

- You must provide an update to at least one **Request** field. Otherwise, this block takes the **Error** branch.

  You can either use an attribute in the Cases namespace, or set the **Request** field manually. If you set manually, see the syntax in [How to persist fields throughout the flow](#).

- Contacts can be routed down the following branches:
  - **Success**: The case was updated, and the contact was linked to the case.
• **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. It might be that the case was updated, but the contact was not linked to the case (partial success/partial failure). If this happens, then the flow will follow this branch.

• **Error**: The case was not updated. The contact was not linked to the case, as the case was not updated.

The following images show an example of an **Update case** configuration. The first image shows that as part of the update the contact is going to be linked to the case. To identify which case to update, the **Case Id** is specified. (Case Id is the unique identifier of the case and the only field you can provide here. Other fields will not work and produce errors.)

The following image shows the **Request field**, where you specify the fields to update the case.

**Properties: Create case**

When configuring properties to create a case:

• You must provide a case template. For more information, see [Create case templates](#).
• Fields that are required appear in the **Required** fields section. You must assign values to them to create a case.

• You must specify the customer to create a case.
  
  • We recommend adding a [Customer profiles] block to the flow before the Cases block. Use the Customer profiles block to get a customer profile with some prefetched data, or create a new customer profile and then use that to create a case.

  • To provide a value for **Customer Id** in the Cases block, configure the fields as shown in the following image, where **Use attribute** is selected, **Type** is set to **Customer**, and **Attribute** is set to **Profile ARN**.

  ![Required fields](image)

  If you are setting the value manually, you must provide the full customer profile ARN in this format:

  ```markdown
  arn:aws:profile:your AWS Region:your AWS account ID:domains/profiles
  domain name/profiles/profile ID
  ```

  • You can specify values for fields other than the required ones in the Request fields section.

  You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in [How to persist fields throughout the flow].

  • You can specify that a contact should be linked to case. If you link the contact to the case, then the contact and a link to contact details appear on the case that the agent sees in the agent application.

  • After creating a case, the case ID that is created will be persisted in the case namespace. It can be used in other blocks by accessing the case namespace case ID attribute value.
• Contacts can be routed down the following branches:

  • **Success**: The case was created, and the contact was linked to the case.

  • **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. This is because it is possible that the case was created, but the contact was not linked to the case (partial success/partial failure). If this happens, then the flow will follow this branch.

  • **Error**: The case was not created. The contact was not linked to the case, as the case was not created.

The following images show an example of a **Create case** configuration. The first image shows the new case will be created using the General inquiry template:

![Create case configuration](image)

The next image shows the reason for the case will be set to **Shipment delayed**.
How to persist fields throughout the flow

Let’s say you want customers to be able to call into your contact center and get the status of their case without ever talking to an agent. You want the IVR to read the status to the customer. You can get the status from a system field, or you might have a custom status field, for example, named *Detailed status*.

Here’s how to configure your flow to get and read the status to the customer:

1. Add a **Cases** block to your flow. Configure it to **Get case** to find the case.
2. In the **Request fields** section, search for the case by the customer **Profile ARN**:

3. In the **Response fields** section, add the field that you want passed throughout the flow. For our example, choose **Status**.
4. Add a **Play prompt** block to your flow.

5. Configure **Play prompt** to set the attribute manually:

Use the following syntax for reading the status of the case to the customer:
• For system fields, you can read the syntax and understand which field it refers to. For example: 
$.Case.status refers to the case status. For a list of system field IDs, see the Field ID column in the System case fields topic.

• For custom fields, the syntax uses a UUID (unique ID) to represent the field. For example, in the following image, the ID for the custom field named Detailed status is 12345678-aaaa-bbbb-cccc-123456789012.

Find the custom field ID

To find the UUID of a custom field:

1. In Amazon Connect, on the navigation menu choose Agent applications, Custom fields, and then choose the custom field that you want.
2. While on the details page for the custom field, look at the URL of the page. The UUID is the last portion of the URL. For example, in the following URL:

https://instance alias.my.connect.aws/cases/configuration/fields/update/12345678-aaaa-bbbb-cccc-123456789012

The UUID is 12345678-aaaa-bbbb-cccc-123456789012.

The following image shows where you find the custom field ID at the end of a URL:
Configuration tips

- Be sure to check the [Cases service quotas](#), and request increases. The quotas apply when this block creates cases.

Configured block

The following image shows an example of what this block looks like when it is configured. It shows this block is configured to create cases, and it has Success and Error branches.

Flow block: Change routing priority / age

Description

- Change a customer's position in the queue. For example, move the contact to the front of the queue, or to the back of the queue.
## Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Flow types

You can use this block in the following flow types:

- Outbound Whisper flow
- Inbound flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

## Properties

The following image shows the Properties page of the Change routing priority / age block. It is configured to add 8 seconds to the routing age of the contact.
This block gives you two options for changing a contact's position in queue:

- **Set priority.** The default priority for new contacts is 5. You can raise the priority of a contact - compared to other contacts in the queue - by assigning them a higher priority, such as 1 or 2.
- **Adjust by time.** You can add or subtract seconds or minutes from the amount of time the current contact spends in queue. Contacts are routed to agents on a first-come, first-served basis. So changing their amount of time in queue compared to others also changes their position in queue.

Here's how this block works:

1. Amazon Connect takes the actual "time in queue" for the contact (in this case, how long this specific contact has spent in queue so far), and adds the number of seconds you specified in the **Adjust by time** property.
2. The additional seconds makes this specific contact look artificially older than it is.
3. The routing system now perceives this contact's "time in queue" as longer than it actually is, which affects its position within the ranked list.

**Configuration tips**

- When using this block, it takes at least 60 seconds for a change to take effect for contacts already in queue.
- If you need a change in a contact's priority to take effect immediately, set the priority before putting the contact in queue, that is, before using a [Transfer to queue](#) block.
Configured block

The following image shows an example of what this block looks like when it is configured. It shows the **Queue time** is set to +8 seconds, and it has a **Success** branch.

![Example of a configured block](image)

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- [Sample customer queue priority](#)
- [Sample queue configurations](#)

Scenarios

See these topics for more information about how routing priority works:

- [Concepts: Routing profiles](#)
- [How routing works](#)

Flow block: Check call progress

⚠️ **Important**

This block works with **outbound campaigns** only.

Description

- Engages with the output provided by an answering machine, and provides branches to route the contact accordingly.
• It supports the following branches:

  • **Call answered**: The call has been answered by a person.

  • **Voicemail (beep)**: Amazon Connect identifies that the call ended in a voicemail and it detects a beep.

  • **Voicemail (no beep)**:
    • Amazon Connect identifies that the call ended in a voicemail but it doesn't detect a beep.
    • Amazon Connect identifies that the call ended in a voicemail, but the beep is unknown.

  • **Not detected**: Could not detect whether there is voicemail. This happens when Amazon Connect is unable to make a positive determination of whether a call was answered by a live voice or an answering machine. Typical situations that land in this state include long silences or excessive background noise.

  • **Error**: If any errors are encountered due to Amazon Connect not running correctly after media has been established on the call, this is the path that will be taken by the flow. Media is established when the call is either answered by a live voice or by an answering machine. If the call is rejected by the network or encounters a system error while placing the outbound call, the flow will not be run.

**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following [flow types]:

• All flow types
Properties

The following image shows the Properties page of the Check call progress block.

Configured block

The following image shows an example of what this block looks like when it is configured. It has branches for Call answered, Voicemail (beep), Voicemail (no beep), Not detected, and Error.

Flow block: Check contact attributes

Description

- Branches based on a comparison to the value of a contact attribute.
- Supported comparisons include: Equals, Is Greater Than, Is Less Than, Starts With, Contains.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.
Flow types

You can use this block in the following flow types:

- All flows

Properties

The following image shows the Properties page of the Check contact attributes block. In this example, the block is configured to check whether the contact is a PremiumCustomer, which is a user-defined attribute.

![Check contact attributes](image-url)
Conditions to check can be dynamic

You can check conditions like the following:

- $.Attributes.verificationCode

To check for a NULL value, you need to use a Lambda.

Amazon Lex attributes

You can set attributes that are **Type** = **Lex** as follows:

- **Alternative Intents**: Usually you configure flows to branch on the winning Lex intent. However, in some situations, you might want to branch on an alternate intent. That is, what the customer might have meant.

For example, in the following image of the **Check contact attributes** properties page, it is configured so the alternative intent indicates that if Amazon Lex is more than 70% confident the customer meant *fraud*, the flow should branch accordingly.

1. **Intent name** is the name of an alternate intent in Lex. It's case sensitive and must match what's in Lex exactly.

2. **Intent Attribute** is what Amazon Connect is going to check. In this example, it's going to check the **Intent Confidence Score**.

3. **Conditions to check**: If Lex is 70% certain the customer meant the alternate intent instead of the winning intent, branch.
• **Intent Confidence Score:** How confident is the bot that it understands the customer's intent. For example, if the customer says "I want to update an appointment," update can mean *reschedule* or *cancel*. Amazon Lex provides the confidence score on a scale of 0 to 1:
  - 0 = not at all confident
  - .5 = 50% confident
  - 1 = 100% confident

• **Intent Name:** The user intent returned by Amazon Lex.

• **Sentiment Label:** What is the winning sentiment, the one with the highest score. You can branch on POSITIVE, NEGATIVE, MIXED, or NEUTRAL.

• **Sentiment Score:** Amazon Lex integrates with Amazon Comprehend to determine the sentiment expressed in an utterance:
  - Positive
  - Negative
  - Mixed: The utterance expresses both positive and negative sentiments.
  - Neutral: The utterance does not express either positive or negative sentiments.

• **Session Attributes:** Map of key-value pairs representing the session-specific context information.

• **Slots:** Map of intent slots (key/value pairs) Amazon Lex detected from the user input during the interaction.

**Configuration tips**

• If you have multiple conditions to compare, Amazon Connect checks them in the order they are listed.

For example, in the following image of the Check contact attributes properties page, it is configured so Amazon Connect compares the *greater than 60* condition first and compares *greater than 2* last.
This block doesn't support case-insensitive pattern matching. For example, if you're trying to match against the word `green` and the customer types `Green`, it would fail. You would have to include every permutation of upper and lower-case letters.

**Configured**

The following image shows an example of what this block looks like when it is configured. It shows the block has four branches, one for each condition: greater or equal to 60, greater to equal to 10, greater or equal to 2, or **No match**.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample inbound flow (first contact experience)
- Sample interruptible queue flow with callback

Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes
- Route based on contact's channel

Flow block: Check hours of operation

Description

- Checks whether the contact is occurring within or outside of the hours of operation defined for the queue.
- Branches based on specified hours of operation.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Check hours of operation block. The block is configured for specific hours of operation.

You can set up multiple hours of operation so you have one for various queues. For instructions, see Set the hours of operation and timezone for a queue.

Configuration tips

- Agent queues that are automatically created for each agent in your instance do not include an hours of operation.
- If you use this block to check the hours of operation for an agent queue, the check fails and the contact is routed down the Error branch.

Configured block

The following image shows an example of what this block looks like when it is configured. It is configured for Basic Hours of operation. It has three branches: In hours, Out of Hours, and Error.
Related topics

- Set the hours of operation and timezone for a queue

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

Sample inbound flow (first contact experience)

Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue

Flow block: Check queue status

Description

- Checks the status of the queue based on specified conditions.
- Branches based on the comparison of Time in Queue or Queue capacity.
  - Time in queue is the amount of time the oldest contact spends in queue, before they are routed to an agent or removed from the queue.
  - Queue capacity is number of contacts waiting in a queue.
- If no match is found, the No Match branch is followed.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Check queue status block. In this example, it checks whether a contact has been in the BasicQueue longer than 2 minutes.
The order in which you add conditions matters at the runtime. Results are evaluated against conditions in the same order in which you add them to the block. Contacts are routed down the first condition to match.

For example, in the following condition order, every value matches one of first two conditions. None of the other conditions are ever matched.

- Time in Queue <= 90
- Time in Queue >= 90
- Time in Queue >= 9
- Time in Queue >= 12
- Time in Queue >= 15
- Time in Queue >= 18
- Time in Queue > 20
- Time in Queue > 21

In this next example, all contacts with a wait time in queue of 90 or less (<=90) match first condition only. This means less than or equal to 9 (<=9), <=12, <=15, <=18, <=20, <=21 are never run. Any value greater than 90 is routed down the greater than or equal to 21 (>=21) condition branch.
- Time in Queue <= 90
- Time in Queue <= 9
- Time in Queue <= 12
- Time in Queue <= 15
- Time in Queue <= 18
- Time in Queue < 20
- Time in Queue < 21
- Time in Queue > 21

**Configured block**

The following image shows an example of what this block looks like when it is configured. It has three branches: the **Time in Queue** condition, **No Match**, and **Error**.

![Configured block example](image)

**Scenarios**

See these topics for scenarios that use this block:

- [Manage contacts in a queue](#)

**Flow block: Check Voice ID**

**Description**

⚠️ **Note**

The [Set Voice ID](#) block needs to be set in the flow before this one. That block sends audio to [Amazon Connect Voice ID](#) to verify the customer's identity, and returns a status.
The **Check Voice ID** block branches based on the results of the voice analysis and the status returned by Voice ID:

### Enrollment status:
- **Enrolled**: The caller is enrolled in voice authentication.
- **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
- **Opted out**: The caller has opted out of voice authentication.

You are not charged for checking enrollment status.

### Voice authentication status:
- **Authenticated**: The caller's identity has been verified. That is, the authentication score is greater than or equal to the threshold (default threshold of 90 or your custom threshold).
- **Not authenticated**: The authentication score is lower than threshold that you configured.
- **Inconclusive**: Unable to analyze a caller's speech for authentication. This is usually because Voice ID did not get the required 10 seconds to provide a result for authentication.
- **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
- **Opted out**: The caller has opted out of voice authentication.

You are not charged if the result is **Inconclusive**, **Not enrolled** or **Opted out**.

### Fraud detection status:
- **High risk**: The risk score meets or exceeds the set threshold.
- **Low risk**: The risk score did not meet the set threshold.
- **Inconclusive**: Unable to analyze a caller's voice for detection of fraudsters in a watchlist.

You are not charged if the result is **Inconclusive**.

---

**Note**

For **Enrollment status** and **Voice authentication**, the **Customer ID** system attribute needs to be set in **Set contact attributes** block because they are acting on a specific customer. You don't need to do this for **Fraud detection** because it's not acting on a specific customer but rather detecting whether the incoming caller matches a fraudster on your watchlist. This
means it's possible for a customer to be successfully authenticated and still have high fraud risk.

**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Inbound flow
- Customer queue flow
- Customer whisper flow
- Outbound whisper flow
- Agent whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

This block doesn't have any properties that you set. Rather, it creates branches for you to route contacts based on the result of the authentication threshold and voiceprint evaluation that Set Voice ID returns.

The following image shows the Properties page for the Check voice ID block when it's configured to check for Enrollment status. Different status results are returned when it's configured for Voice authentication or Fraud detection.
Configuration tips

When you create a flow that uses this block, add these blocks in the following order:

1. **Set Voice ID** block.
2. **Set contact attributes** block: For **Enrollment status** and **Voice authentication**, the **Customer ID** system attribute needs to be set in **Set contact attributes** block because it is acting on a specific customer.
3. **Check Voice ID** block.

Configured block

The following three images show what this block looks like when it's configured to check for:

1. Enrollment status
2. Voice authentication
3. Fraud detection
More information

See the following topics for more information about this block:

- Use real-time caller authentication with Voice ID
- Use Voice ID

Flow block: Check staffing

Description

- Checks the current working queue, or queue you specify in the block, for whether agents are available, staffed, or online.
- Before transferring a call to agent and putting that call in a queue, use the Check hours of operation and Check staffing blocks. They verify that the call is within working hours and that agents are staffed to service.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.
<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Inbound flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

The following image shows the Properties page of the Check staffing block. It is configured to check whether agents in the BasicQueue have slots available so they can be routed contacts.
In the **Status to check** dropdown box, choose one of the following options:

- **Available** = Check whether the agent has **Available** slots to be routed a contact.
- **Staffed** = Check whether agents have **Available** slots, or are **On call**, or are in **After Contact Work**.
- **Online** = Check whether agents are **Available**, in the **Staffed** state, or in a custom state.

**Configuration tips**

- You must set a queue before using a **Check staffing** block in your flow. You can use a **Set working queue** block to set the queue.
- If a queue is not set, the contact is routed down the **Error** branch.
- When a contact is transferred from one flow to another, the queue that is set in a flow is passed from that flow to the next flow.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It has three branches: **True**, **False**, and **Error**.

![Check staffing block](image)

**Scenarios**

See these topics for scenarios that use this block:

- **Transfer contacts to a specific agent**
Flow block: Create persistent contact association

Description

- Enables persistent chat experience on the current chat.
- This allows you to select the required rehydration mode. For more information about chat rehydration, see Enable persistent chat.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Customer hold flow
- Customer whisper flow
- Outbound whisper flow
- Agent hold flow
- Agent whisper flow
- Transfer to agent flow
- Transfer to queue flow
Properties

The following image shows the Properties page of the Create persistent contact association block.

**Configuration tips**

- To enable persistent chat you can add the Create persistent contact association block to your flow, or provide the previous contactId in the SourceContactId parameter of the StartChatContact API, but not both. You can enable persistence of a SourceContactID on a new chat only once.
We recommend that you enable persistent chat by using the **Create persistent contact association** block when using the following features:

- [Amazon Connect chat widget](#)
- [Apple Messages for Business](#)

You can configure persistent chats to rehydrate the entire past chat conversation or rehydrate from a specific segment of a past chat conversation. For information about rehydration types, see [Enable persistent chat](#).

### Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: **Success** and **Error**.

![Create persistent contact association](image)

### Flow block: Create task

**Description**

- Creates a new task manually or by leveraging a [task template](#).
- Sets the tasks attributes.
- Initiates a flow to start the task immediately or schedules it for a future date and time.

For more information about Amazon Connect Tasks, see [Concepts: Tasks in Amazon Connect](#).
Note

If your Amazon Connect instance was created on or before October 2018, the contact is routed down the error branch. For the contact to be routed down the success path, create an IAM policy with the following permission and attach it to the Amazon Connect service role. You can find the Amazon Connect service role on the Account overview page for your Amazon Connect instance.

```json
{
   "Effect": "Allow",
   "Action": "connect:StartTaskContact",
   "Resource": "*"
}
```

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- All flows

Properties

When you configure a Create task block, you choose either Create manually or Use template. Your choice dictates which fields you'll need to complete on the rest of Properties page. Following is more information about these two options.
Option 1: Create manually

The following image shows the Properties page when Create manually is selected. All settings on the page can be specified manually or dynamically.

If you choose Use template at bottom of the page, the entire page switches to that option. If needed, you can toggle back to Create manually and continue with your manual settings.

Option 2: Use template

After you create a template, it's available for you to specify it in Create task block.

The following image shows the Properties page when Use template is selected. In this example, the name of the template is Test Template. Notice that Test Template does not include a flow.

- If the selected template does not include a flow, you must specify the flow that you want the task to run.
- You cannot overwrite the settings of any fields on the page that are populated by the template.
Configuration tips

- The **Create task** block branches based on whether the task was successfully created:
  - **Success** if task was created. It responds with the contact ID of the newly created task.
  - **Error** if task wasn't created.
- **Referencing a task contact ID**: The newly created task runs the flow that you specified in the **Flow** section of the block, or it runs the flow configured by the task template that you selected. You can reference the contact ID of the newly created task in subsequent blocks.

For example, you might want to reference the task contact ID in the **Play prompt** block. You can specify the task contact ID dynamically by using the following attribute:

- **Namespace**: System
- **Value**: Task Contact id

- **Scheduling a task**: When you **Set date and time using attribute**: Values for date fields must be in Unix timestamp (Epoch seconds). Because of this, it's most likely that you'll choose a **User-defined** attribute for the **Namespace**.
For example, your flow might have a **Set contact attributes** block that sets a user-defined attribute with key named `scheduledTaskTime`. Then, in the **Create task** block, you would select **User-defined**, and the key would be `scheduledTaskTime`.

To continue with this example, the value in `scheduledTaskTime` must be specified Unix timestamp. For example, 1679609303 is the Unix timestamp that corresponds to Thursday, March 23, 2023 10:08:23 PM UTC.

When the date and time have passed, contacts are always routed down the **Error** branch. To avoid the **Error** branch, be sure to keep the Epoch seconds updated to a valid date and time in the future.

- Be sure to check the [service quotas](#) for tasks and API throttling, and request increases, if needed. The quotas apply when this block creates tasks.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It has two branches: **Success** and **Error**.

![Configured block](image)

**Sample flows**

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- [Sample inbound flow (first contact experience)](#)
Flow block: Customer profiles

Description

- Enables you to retrieve, create, and update a customer profile.
  - You can configure the block to retrieve profiles using up to five search identifiers of your choice.
- Enables you to retrieve a Customer Profile's object and calculated attributes.
  - You can configure the block to retrieve objects using a search identifier of your choice.
  - You must provide a profile ID in this block. You can provide a profileID manually, or use the profileID saved in the Customer namespace after you have found a profile using the Get profile action.
- Enables you to associate the contact, such as voice, chat, and tasks, to an existing customer profile.
- When customer profile data is retrieved, the Response fields are stored in the contact attributes for that customer, allowing you to use them in subsequent blocks.

The following examples show how you might use this block:

- Use a Play prompt block after retrieving a profile to provide a personalized call or chat experience by referencing the supported profile fields.
- Use a Check contact attributes block after retrieving profile data to route a contact conditional on the value.
- See How to persist fields throughout the flow for more details.

Supported channels

The following table lists how this block routes a contact that is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Channel</td>
<td>Supported?</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- All flow types

**Configuration tips**

- Before using this block, make sure Customer Profiles is enabled for your Amazon Connect instance. For instructions, see [Use Customer Profiles](#).

- A contact is routed down the **Error** branch in the following situations:
  - Customer Profiles is not enabled for your Amazon Connect instance.
  - Request data values are not valid. The request values cannot be over 255 characters.
  - The Customer Profiles API request has been throttled.
  - Customer Profiles is having availability issues.

- The total size of [Customer Profiles contact attributes](#) is limited to 14,000 characters (56 attributes assuming max size of 255 each) for the entire flow. This includes all values persisted as **Response fields** in Customer Profiles blocks during the flow.

**Properties**

The following property types are available in the Customer Profiles flow block:

- [Get Profile](#)
- [Create Profile](#)
- [Update Profile](#)
- [Get Profile Object](#)
- [Get Calculated Attributes](#)
- [Associate Contact to Profile](#)
Properties: Get profile

When configuring properties to Get profile, consider the following:

- You must provide at least one search identifier, up to five total.
- If multiple search identifiers are provided, you must provide one logical operator, either AND or OR. The logical operator will be applied across all search identifiers like one of the expressions shown below
  - i.e. (a AND b AND c)
  - i.e. (x OR y OR z)
- Define attributes to persist in subsequent blocks, storing them in contact attributes under Response fields.
- Contacts can be routed down the following branches
  - Success: one profile was found. Response fields are stored to contact attributes
  - Error: An error was encountered while trying to find the profile. This may be due to a system error or how Get profile is configured.
  - Multiple Found: multiple profiles were found.
  - None Found: no profile was found.

The following image shows an example of a Customer Profiles Properties page that is configured for the Get profile action.

The displayed block is configured to search for profiles that either match the caller's Phone number or share the same Account number stored in the user-defined attribute named "Account." When one profile is located, the Response fields - AccountNumber, FirstName, LastName, PhoneNumber, and Attributes.LoyaltyPoints - are stored in the contact attributes for that specific customer.
Select an action

Get profile

Search identifiers

Use search identifiers to find a profile.

- Phone = $.CustomerEndpoint.Address
  OR
- Account = $.Attributes.Account

+ Add another search identifier

Select logical operator

Search identifier

OR

Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

Response fields

AccountNumber, FirstName, LastName, PhoneNumber, Custom attribute

AccountNumber | FirstName | LastName | PhoneNumber | Custom attribute

Add another custom response field

Key
LoyaltyPoints

Cancel Save
Properties: Create profile

When configuring properties for Create profile, consider the following:

- Specify the attributes you intend to populate during profile creation in the Request fields.
- Define attributes to persist in subsequent blocks, storing them in contact attributes under Response fields.

Contacts can be routed down the following branches:

- **Success**: A profile is successfully created, and Response fields are stored in contact attributes.
- **Error**: An error occurred during the profile creation process, possibly due to a system error or misconfiguration of the Create profile action.

The displayed block below is configured to create a profile with a PhoneNumber and a custom attribute named “Language”. Following the profile creation, the Attributes.Language response field is stored in contact attributes, making it available for use in subsequent blocks.
Select an action

Action
Create profile

Request fields

Request fields

Phone number

Remove

Use custom attributes

Custom attributes

- Language = $.Attributes.Language

+ Add another custom attribute

Request field values

Phone number

Set manually

Set dynamically

Namespace
System

Key
Customer number

Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

Response fields

Custom attribute

Remove

Key
Language

Add another custom response field
Properties: Update profile

When configuring properties to **Update profile**, consider the following:

- Prior to using an **Update profile** block, use a **Get profile** block, as illustrated in the following image. Utilize the **Get profile** block to locate the specific profile you intend to update.

![Diagram of Update profile process](image)

- Provide the attributes and values you wish to update the profile with **Request fields** and **Request field values**.

- Define attributes to persist in subsequent blocks, storing them in contact attributes under **Response fields**.

Contacts can be routed down the following branches:

- **Success**: The profile has been successfully updated, and **Response fields** are stored in contact attributes.

- **Error**: An error occurred during the attempt to update the profile. This could result from a system error or misconfiguration of the **Update profile** action.
The displayed block below is configured to update a Profile with a **MailingAddress1** with user input as value. When a profile is updated, the **MailingAddress1** response field is stored in contact attributes, making it available for use in subsequent blocks.
Select an action

Action
Update profile

Request fields

Request fields
Mailing address 1

Use custom attributes

Request field values

Mailing address 1

Set manually
Set dynamically

Namespace
User defined

Key
address

Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

Response fields
MailingAddress1

Cancel  Save
Properties: Get profile object

When configuring properties to **Get profile object**, consider the following:

- **Mandatory Profile ID**: A Profile ID is required for this block to function. The **Get profile object** action retrieves an object associated with the provided **ProfileID**. Ensure you provide the **ProfileID** by using a preceding **Get profile** block, as illustrated in the following image. Use the **Get profile** block to pinpoint the specific profile before moving forward to retrieve the profile's object in the subsequent block.

- You have the option to manually input the Profile ID or utilize a pre-defined value stored in a pre-defined or user attribute.

- You must indicate the object type from which you intend to retrieve information.

- You must choose one of the following options for object retrieval:
  - **Use latest profile object**: This option consistently retrieves the most recent object.
  - **Use search identifier**: This option involves searching for and retrieving the object using the provided search identifier.

- Define attributes to persist in subsequent blocks, storing them in contact attributes under **Response fields**.
Contacts can be routed down the following branches:

- **Success:** The profile object is successfully located, and **Response fields** are stored in contact attributes.
- **Error:** An error occurred during the attempt to retrieve the profile object. This may be due to a system error or misconfiguration of the **Get Profile** action.
- **None Found:** no object is found.

The displayed block below is configured to retrieve a profile object of type "Asset" associated with the **ProfileId** saved under the "Customer" namespace. In this specific scenario, the block is will search for an Asset using the Asset ID. Once the Asset is located, **Asset.Price** and **Asset.PurchaseDate** are stored in contact attributes, making them available for subsequent blocks.
Customer profiles

Get profile object

Profile ID

- Set manually
- Set dynamically

Object type

- Set manually
  - Object type
    - Asset
- Set dynamically

Get profile object

- Use latest profile object
- Use search identifier

Search identifier

- Set manually
  - Search identifier
    - Asset ID
- Set dynamically

Identifier value

- Set manually
- Set dynamically

Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

Response fields

- Price
- PurchaseDate
Properties: Get calculated attributes

⚠️ Important
To use this action, your Amazon Connect instance must have permission for the following APIs: ListCalculatedAttributeDefinitions and GetCalculatedAttributeForProfile in either of the following Policies: AmazonConnectServiceLinkedRolePolicy or AmazonConnectServiceCustomerProfileAccess.

When configuring properties to Get calculated attributes, consider the following:

- **Mandatory Profile ID**: A Profile ID is required for this block to function. The Get calculated attributes action retrieves an object associated with the provided ProfileID. Ensure you provide the ProfileID by using a preceding Get profile block, as illustrated in the following image. Use the Get profile block to pinpoint the specific profile before moving forward to retrieve the profile’s calculated attributes in the subsequent block.

- You have the option to manually input the Profile ID or utilize a pre-defined value stored in a pre-defined or user attribute.
• Define attributes to persist in subsequent blocks, storing them in contact attributes under **Response fields**.

• The options under **Response fields** are the Calculated Attribute definitions defined for your Customer Profiles domain

• If the definition of calculated attributes uses a threshold, the calculated attribute value will be a Boolean and either return a True/False. Otherwise, they will return a numeric or string value. The return value of the calculated attribute can be utilized for branching purposes in a **Check Contact Attributes** block using conditions such as **Equals**, **Is greater than**, **Is less than**, and **Contains**.

Contacts can be routed down the following branches:

• **Success**: A calculated attribute is found, and Response fields are stored in contact attributes.

• **Error**: An error occurred while attempting to retrieve the calculated attribute. This may be due to a system error or misconfiguration of the **Get calculated attribute** action.

• **None Found**: no calculated attribute is found.

The displayed block below is configured to get calculated attributes belonging to the provided **ProfileId** in contact attributes. The following **Response fields** will be retrieved and stored in contact attributes: **Average Call Duration**, and **Frequent Caller**.
Select an action

Action
Get calculated attributes

Profile ID

- Set manually
- Set dynamically

Namespace
Customer

Key
Profile ID

Calculated attributes

Calculated attributes
Average Call Duration, Frequent Caller

Average Call Duration
Frequent Caller
Properties: Associate contact to profile

⚠️ Important
To use this action, your Amazon Connect instance must have permission for the following APIs: ListCalculatedAttributeDefinitions and GetCalculatedAttributeForProfile in either of the following Policies: AmazonConnectServiceLinkedRolePolicy or AmazonConnectServiceCustomerProfileAccess.

To use this action, you must also enable the Customer Profiles View permission in your security profile.

When configuring properties to Associate contact to profile, consider the following:

- Add a Get profile block before an Associate contact to profile, as shown in the following image. Use the Get profile block to find the profile first, then associate the contact and profile in the next block.

- **Mandatory Profile ID:** A Profile ID is required for this block to function. Ensure you provide the ProfileID by using a preceding Get profile block, as illustrated in the following image. Use the Get profile block to pinpoint the specific profile you wish to associate the contact to in the next block.

- You have the option to manually input the Profile ID or utilize a pre-defined value stored in a pre-defined or user attribute.
• You must provide a value for Contact ID.

Contacts can be routed down the following branches:

• **Success**: Associated the contact to profile.

• **Error**: An error was encountered while attempting to associate the contact to profile. This may be due to a system error or misconfiguration of the Associate contact to profile action.

The displayed block below is configured to associate the profile with **Profile ID** stored in contact attributes to the current Contact ID stored in contact attributes.
**Select an action**

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate contact to profile</td>
</tr>
</tbody>
</table>

To associate contact information with this profile, make sure you’re using the ID you set previously through a Get profile action or a Lambda function.

**Profile ID**

- [ ] Set manually
- [x] Set dynamically

<table>
<thead>
<tr>
<th>Namespace</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile ID</td>
<td></td>
</tr>
</tbody>
</table>

**Contact ID**

- [ ] Set manually
- [x] Set dynamically

<table>
<thead>
<tr>
<th>Namespace</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact id</td>
<td></td>
</tr>
</tbody>
</table>
How to persist fields throughout the flow

Let's say you want customers to interact with your contact center and learn the status of their delivery order without directly communicating with an agent. Additionally, let's say you want to prioritize incoming calls from customers who have experienced more than 10 minutes delay in the past.

In these scenarios, the IVR needs to fetch the relevant information about the customer. This is achieved through the Customer Profiles block. Secondly, the IVR needs to leverage this customer data in other Flow blocks in order to personalize the experience and proactively service the customer.

1. Use **Play Prompt** to personalize the experience by greeting the customer by name and informing them of their status.
Block Type

Play prompt

Block Name

Enter a block name

Delivers an audio or chat message. Learn more

- Select from the prompt library (audio)
- Specify an audio file from an S3 bucket
- Text-to-speech or chat text
  - Set manually

Enter text to be spoken


- Set dynamically

Interpret as

Text
2. Use **Check contact attributes** to conditionally route customers based on their Average Hold Time from previous interactions
Block Type

Check contact attributes

Block Name

Enter a block name

Branches based on a comparison to the value of a contact attribute. Learn more

Attribute to check

Namespace

Customer

Key

Calculated Attributes

Key

Average Hold Time

Conditions to check

condition

Is greater than

value

10

Add another condition

No Match
Configured block

The following image shows an example of what this block looks like when it is configured. It shows four branches: Success, Error, Multiple found, and None found.

Flow block: Disconnect / hang up

Description

- Disconnects the contact.

Supported channels

The following table lists how this block routes a contact that is using the specified channel.
Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Flow block: Distribute by percentage

Description

- This block is useful for doing A/B testing. It routes customers randomly based on a percentage.
- Contacts are distributed randomly, so exact percentage splits may or may not occur.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Distribute by percentage
Flow types

You can use this block in the following flow types:

• Inbound flow
• Customer queue flow
• Outbound Whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the Distribute by percentage block. It is configured to route 50% of contacts to the test branch.

How it works

This block creates static allocation rules based on how you configure it. Internal logic generates a random number between 1-100. This number identifies which branch to take. It doesn't use current or historical volume as part of it's logic.

For example, say a block is configure like this:

• 20% = A
• 40% = B
• 40% remaining = Default
When a contact is being routed through a flow, Amazon Connect generates a random number.

- If the number is between 0-20, the contact is routed down the A branch.
- Between 21-60 it's routed down the B branch.
- Greater than 60 it's routed down the Default branch.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It shows two branches: **50% test** and **50% default**.

![Configured block example](image)

**Sample flows**

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- **Sample AB test**

**Flow block: End flow / Resume**

**Description**

- Ends the current flow without disconnecting the contact.
- This block is often used for the **Success** branch of the **Transfer to queue** block. The flow doesn't end until the call is picked up by an agent.
- You also might use this block when a **Loop prompts** block is interrupted. You can return the customer to the **Loop prompts** block.

**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.
<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Customer queue flow
- Customer whisper flow
- Outbound Whisper flow
- Agent whisper flow

**Properties**

The following image shows the Properties page of the End flow / Resume block.

![Properties page](image)

**Configured block**

The following image shows an example of what this block looks like when it is configured. It does not have any The End flow / Resume termination event branches.
Flow block: Get customer input

Description

- It plays a prompt to get a response from the customer. For example, "For Sales, press one. For Support, press two."
- When customers enter DTMF input (touch-tone keypad or telephone input), the prompt is interruptible.
- When an Amazon Lex bot plays a voice prompt, customers can interrupt it with their voice. To set this up, use the barge-in-enabled session attribute.
- It then branches based on the customer's input.
- This block works for chat only when Amazon Lex is used. It gathers customer input only, not agent input.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Chat    | Yes when Amazon Lex is used  
|         | Otherwise, No - Error branch |
| Task    | Yes                      |

Flow types

You can use this block in the following flow types:
• Inbound flow
• Customer queue flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the Get customer input block. It is configured to play an audio prompt. It branches on DTMF input, and times out after 5 seconds if the customer doesn't enter anything.

Note

The Get Customer Input block does not currently support using a voice prompt from an S3 bucket with Amazon Lex V2.

For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the Play prompt block.

You can configure this block to accept DTMF input or a chat response. You can also configure it work with Amazon Lex; for example, a contact can be routed based on their utterance. To learn how to set up a Lex bot, see Tutorial 3: Create an IT help desk.
**DTMF tab properties**

- **Audio prompt**: Select from a list of default audio prompts, or upload your own audio prompt.
- **Set timeout**: Specify how long to wait while the user decides how they want to respond to the prompt. The maximum timeout you can set is 179 seconds.

**Amazon Lex tab properties**

Amazon Lex

ℹ️ **Note**

Your language attribute in Amazon Connect must match the language model used to build your Amazon Lex V2 bot. Set the language attribute using the Set voice block or the Set contact attributes block.

- **Lex bot properties**: After you create your Lex bot, enter the name and alias of the bot here. Only built bots appear in the drop-down list.

The following image shows the Amazon Lex tab configured to use a Lex bot named **Help Desk (US West: Oregon)**.
Important

In a production environment, always use a different alias than TestBotAlias for Amazon Lex and $LATEST for Amazon Lex classic. TestBotAlias and $LATEST support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime quotas or Runtime Service Quotas (Amazon Lex Classic).

- **Session attributes**: Specify attributes that apply to the current contact's session only. The following image shows the session attributes configured for a max speech duration of 8000 milliseconds (8 seconds).

![Session attributes](image)

- **Use sentiment override**: Branch based on sentiment score, before the Amazon Lex intent.

  The sentiment score is based on the last utterance of the customer. It is not based on the entire conversation.

  For example, a customer calls and they have a negative sentiment because their preferred appointment time isn't available. You can branch the flow based on their negative sentiment score, for example, if their negative sentiment is more than 80%. Or, a customer calls and has a positive sentiment of more than 80%, you can branch to upsell them on services.

  The following image shows the Intents section of the Amazon Lex tab. It is configured to route the contact when their negative sentiment score is 80%.
If you add both negative and positive sentiment scores, the negative score is always evaluated first.

For information about how to use sentiment score, alternative intents, and sentiment label with contact attributes, see Check contact attributes.

Amazon Lex (Classic)

- **Lex bot properties**: After you create your Lex bot, enter the name and alias of the bot here. Only published bots appear in the drop-down list.

The following image shows the Amazon Lex tab configured to use a Lex bot named Help Desk (US West: Oregon).
In a production environment, always use a different alias than TestBotAlias for Amazon Lex and $LATEST for Amazon Lex classic. TestBotAlias and $LATEST support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime quotas or Runtime Service Quotas (Amazon Lex Classic).

- **Session attributes**: Specify attributes that apply to the current contact's session only.

The following image shows the session attributes configured for a max speech duration of 8000 milliseconds (8 seconds).
Configurable time-outs for voice input

To configure time-out values for voice contacts, use the following session attributes in the Get customer input block that calls your Lex bot. These attributes allow you to specify how long to wait for the customer to finish speaking before Amazon Lex collects speech input from callers, such as answering a yes/no question, or providing a date or credit card number.

Amazon Lex

- **Max Speech Duration**

  x-amz-lex:audio:max-length-ms:[intentName]:[slotToElicit]

  How long the customer speaks before the input is truncated and returned to Amazon Connect. You can increase the time when a lot of input is expected or you want to give customers more time to provide information.

  Default = 12000 milliseconds (12 seconds). The maximum allowed value is 15000 milliseconds.

  ! Important

  If you set Max Speech Duration to more than 15000 milliseconds, the contact is routed down the Error branch.

- **Start Silence Threshold**

  x-amz-lex:audio:start-timeout-ms:[intentName]:[slotToElicit]

  How long to wait before assuming that the customer isn't going to speak. You can increase the allotted time in situations where you'd like to allow the customer more time to find or recall information before speaking. For example, you might want to give customers more time to get out their credit card so they can enter the number.

  Default = 3000 milliseconds (3 seconds).

- **End Silence Threshold**

  x-amz-lex:audio:end-timeout-ms:[intentName]:[slotToElicit]
How long to wait after the customer stops speaking before assuming the utterance has concluded. You can increase the allotted time in situations where periods of silence are expected while providing input.

Default = 600 milliseconds (0.6 seconds)

Amazon Lex (Classic)

- **Max Speech Duration**

  `x-amz-lex:max-speech-duration-ms:[intentName]:[slotToElicit]`

  How long the customer speaks before the input is truncated and returned to Amazon Connect. You can increase the time when a lot of input is expected or you want to give customers more time to provide information.

  Default = 12000 milliseconds (12 seconds). The maximum allowed value is 15000 milliseconds.

  **Important**

  If you set **Max Speech Duration** to more than 15000 milliseconds, the contact is routed down the **Error** branch.

- **Start Silence Threshold**

  `x-amz-lex:start-silence-threshold-ms:[intentName]:[slotToElicit]`

  How long to wait before assuming that the customer isn't going to speak. You can increase the allotted time in situations where you'd like to allow the customer more time to find or recall information before speaking. For example, you might want to give customers more time to get out their credit card so they can enter the number.

  Default = 3000 milliseconds (3 seconds).

- **End Silence Threshold**

  `x-amz-lex:end-silence-threshold-ms:[intentName]:[slotToElicit]`
How long to wait after the customer stops speaking before assuming the utterance has concluded. You can increase the allotted time in situations where periods of silence are expected while providing input.

Default = 600 milliseconds (0.6 seconds)

**Configurable time-outs for chat input during a Lex interaction**

Use the **Chat timeout** field under **Intents** to configure timeouts for chat input. Enter how long until inactive customers timeout in a Lex interaction.

- Minimum: 1 minute
- Maximum: 7 days

The following image shows the **Get customer input** block configured to timeout chats when the customer is inactive for 2 minutes.

For information about setting up chat timeouts when all participants are human, see [Set up chat timeouts for chat participants](#).

**Barge-in configuration and usage for Amazon Lex**

You can allow customers to interrupt the Amazon Lex bot mid-sentence using their voice, without waiting for it to finishing speaking. Customers familiar with choosing from a menu of options, for example, can now do so without having to listen to the entire prompt.

Amazon Lex

- **Barge-in**
Barge-in is enabled globally by default. You can disable it in the Amazon Lex console. For more information, see Enabling your bot to be interrupted by your user. Additionally, you can modify barge-in behavior, by using the allow-interrupt session attribute. For example, x-amz-lex:allow-interrupt:*:* allows interrupt for all intents and all slots. For more information, see Configuring timeouts for capturing user input in the Amazon Lex V2 Developer Guide.

Amazon Lex (Classic)

- **Barge-in**

  x-amz-lex:barge-in-enabled:[intentName]:[slotToElicit]

Barge-in is disabled globally by default. You must set the session attribute in the Get customer input block that calls your Lex bot to enable it at the global, bot, or slot levels. This attribute only controls Amazon Lex barge-in; it doesn't control DTMF barge-in. For more information, see How to use Lex session attributes.

The following image shows the Session attributes section with barge-in enabled.

![Session attributes image]

**Configurable fields for DTMF input**

Use the following session attributes to specify how your Lex bot responds to DTMF input.

- **End character**

  x-amz-lex:dtmf:end-character:[IntentName]:[SlotName]
The DTMF end character that ends the utterance.

Default = #

- **Deletion character**

  x-amz-lex:dtmf:deletion-character:[IntentName]:[SlotName]

  The DTMF character that clears the accumulated DTMF digits and ends the utterance.

  Default = *

- **End timeout**

  x-amz-lex:dtmf:end-timeout-ms:[IntentName]:[SlotName]

  The idle time (in milliseconds) between DTMF digits to consider the utterance as concluded.

  Default = 5000 milliseconds (5 seconds)

- **Max number of allow DTMF digits per utterance**

  x-amz-lex:dtmf:max-length:[IntentName]:[SlotName]

  The maximum number of DTMF digits allowed in a given utterance. This cannot be increased.

  Default = 1024 characters

For more information, see [How to use Lex session attributes](#).

**Intents**

- Enter the intents you created in Amazon Lex. They are case sensitive!

  The following image shows two intents in the Intents section: PasswordReset and NetworkIssue.
Configuration tips

- This topic explains some of the session attributes available for the integration with Amazon Lex. For a list of all the available Amazon Lex session attributes, see Configuring timeouts for capturing user input.

- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters (6,000 total characters).

- Amazon Lex bots support both spoken utterances and keypad input when used in a flow.

- For both voice and DTMF, there can be only one set of session attributes per conversation. Following is the order of precedence:
  1. Lambda provided session attributes: Overrides to session attributes during customer Lambda invocation.
  2. Amazon Connect console provided session attributes: Defined in the Get customer input block.
  3. Service defaults: These are used only if no attributes are defined.

- You can prompt contacts to end their input with a pound key # and to cancel it using the star key *. When you use a Lex bot, if you don’t prompt customers to end their input with #, they will end up waiting five seconds for Lex to stop waiting for additional key presses.

- To control time-out functionality, you can use Lex session attributes in this block, or in set them in your Lex Lambda function. If you choose to set the attributes in a Lex Lambda function, the default values are used until the Lex bot is invoked. For more information, see Using Lambda Functions in the Amazon Lex Developer Guide.
When you specify one of the session attributes described in this article, you can use wildcards. They let you set multiple slots for an intent or bots.

Following are some examples of how you can use wildcards:

- To set all slots for a specific intent, such as PasswordReset, to 2000 milliseconds:

  Name = x-amz-lex:max-speech-duration-ms:PasswordReset:*

  Value = 2000

- To set all slots for all bots to 4000 milliseconds:

  Name = x-amz-lex:max-speech-duration-ms:*:*

  Value = 4000

Wildcards apply across bots but not across blocks in a flow.

For example, you have a Get_Account_Number bot. In the flow, you have two Get customer input blocks. The first block sets the session attribute with a wildcard. The second one doesn't set the attribute. In this scenario, the change in behavior for the bot applies only to the first Get customer input block, where the session attribute is set.

- Because you can specify that session attributes apply to the intent and slot level, you can specify that the attribute is set only when you're collecting a certain type of input. For example, you can specify a longer Start Silence Threshold when you're collecting an account number than when you're collecting a date.

- If DTMF input is provided to a Lex bot using Amazon Connect, the customer input is made available as a Lex request attribute. The attribute name is x-amz-lex:dtmf-transcript and the value can be a maximum of 1024 characters.

Following are different DTMF input scenarios:

<table>
<thead>
<tr>
<th>Customer input</th>
<th>DTMF transcript</th>
</tr>
</thead>
<tbody>
<tr>
<td>[DEL]</td>
<td>[DEL]</td>
</tr>
<tr>
<td>[END]</td>
<td>[END]</td>
</tr>
<tr>
<td>123[DEL]</td>
<td>[DEL]</td>
</tr>
</tbody>
</table>
Customer input | DTMF transcript
---|---
123[END] | 123

Where:
- [DEL] = Deletion character (Default is *)
- [END] = End character (Default is #)

**Problems with DTMF input?**

Let's say you have the following scenario with two contacts flows, each one capturing DTMF input from customers:

1. One flow uses the **Get customer input** block to request DTMF input from customers.
2. After the DTMF input is entered, it uses the **Transfer to flow** block to move the contact to the next contact flow.
3. In the next flow, there's a **Store customer input** block to get more DTMF input from the customer.

There's setup time between the first and second flows. This means if the customer enters DTMF input very quickly for the second flow, some of the DTMF digits might be dropped.

For example, the customer needs to press 5, then wait for a prompt from the second flow, then type 123. In this case, 123 is captured without problem. However, if they don't wait for the prompt and enter 5123 very quickly, the **Store customer input** block may capture only 23 or 3.

To guarantee the **Store customer input** block in second contact flow captures all of the digits, the customer needs to wait for the prompt to be played, and then enter their type DTMF input.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It shows two branches for DTMF input: **Pressed 1** and **Pressed 2**. It also shows branches for **Timeout**, **Default**, and **Error**.
1. **Timeout**: What to do when the time in the **Set timeout** property has elapsed.

2. **Default**: What to do if a customer enters a value other than 1 or 2.

### Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- [Sample inbound flow (first contact experience)](#)
- [Sample interruptible queue flow with callback](#)
- [Sample queue configurations](#)
- [Sample recording behavior](#)

### Scenarios

See these topics for scenarios that use this block:

- [Add an Amazon Lex bot to Amazon Connect](#)
- [How to use the same bot for voice and chat](#)
- [Add text-to-speech to prompts](#)
Flow block: Get queue metrics

Description

- Retrieves near real-time metrics, with a delay of 5-10 seconds, from a queue so you can make routing decisions. If there is no current activity in your contact center, nothing is returned for these metrics.

Following are the metrics that can be retrieved:

- Queue name
- Queue ARN.
- Contacts in queue
- Oldest contact in queue
- Agents online
- Agents available
- Agents staffed
- Agents after contact work
- Agents busy: Although this option maps to the On contact real-time metric, note that On contact includes ACW but Agents busy does not.
- Agents missed (Agent non-response)
- Agents non-productive

- You can choose to return metrics by channel, for example, voice or chat. You can also filter by queue or agent. These options enable you to know how many chat and voice contacts are in a queue and if you have agents available to handle those contacts.

- You can route contacts based on queue status, such as number of contacts in queue or agents available. Queue metrics are aggregated across all channels and are returned as attributes. The current queue is used by default.

- After a Get queue metrics block, use a Check contact attributes to check metric values and define routing logic based on them, such as number of contacts in a queue, number of available agents, and oldest contact in a queue.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.
<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- All flows

**Properties**

The following image shows the Properties page of the Get queue metrics block. It is configured to retrieve metrics for the Voice channel.

You can retrieve metrics by channel, and/or by queue or agent.

- If you don't specify a channel, it returns metrics for all channels.
- If you don't specify a queue, it returns metrics for the current queue.
• Dynamic attributes can only return metrics for one channel.

For example, the following image shows the Properties page configured for the Chat channel and BasicQueue. If you choose these settings Get queue metrics would return metrics for only the BasicQueue, filtered to include only chat contacts.

![Configuration tips](image)

**Configuration tips**

**Specifying a channel in the Set contact attributes block**

Dynamic attributes can only return metrics for one channel.

Before you use dynamic attributes in the Get queue metrics block, you need to set the attributes in the Set contact attributes block, and specify which channel.

When you set a channel dynamically using text, as shown in the following image, for the attribute value enter **Voice** or **Chat**. This value is not case-sensitive.
Using the Check contact attributes block after the Get queue metrics block

After a Get queue metrics block, add a Check contact attributes block to branch based on the returned metrics. Use the following steps:

1. After Get queue metrics, add a Check contact attributes block.
2. In the Check contact attributes block, set Attribute to check to Queue metrics.
3. In the Value dropdown box, you'll see a list of queue metrics that can be checked by the Get queue metrics block. Choose the metric that you want to use for the routing decision.
Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: **Success** and **Error**.

![Configured block diagram]

### Scenarios

See these topics for scenarios that use this block:

- [How to reference contact attributes](#)

### Flow block: Hold customer or agent

#### Description

- Places a customer or agent on or off hold. This is useful when, for example, you want to put the agent on hold while the customer enters their credit card information.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

### Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>
Flow types

You can use this block in the following flow types:

- Inbound flow
- Outbound Whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Hold customer or agent block. It shows that the dropdown list has three options: Agent on hold, Customer on hold, and Conference all.

These options are defined as follows:

- **Agent on hold** = customer is on the call
- **Conference all** = agent and customer are on the call
- **Customer on hold** = agent is on the call

Configured block

The following image shows an example of what this block looks like when it is configured. It configured for **Agent on hold**, and it has two branches: **Success** and **Error**.
Samples flows

Sample secure input with agent

Flow block: Invoke AWS Lambda function

Description

- Calls AWS Lambda, and optionally returns key-value pairs.
- The returned key-value pairs can be used to set contact attributes.
- For an example, see Tutorial: Create a Lambda function and invoke in a flow.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Customer Hold flow
• Customer Whisper flow
• Agent Hold flow
• Agent Whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the AWS Lambda function block.

![Properties Page](image)

Note the following properties:

- **Timeout**: Enter how long to wait for Lambda to time out.

  If your Lambda invocation gets throttled, the request is retried. It is also retried if a general service failure (500 error) happens.

  When a synchronous invocation returns an error, Amazon Connect retries up to three times, for a maximum of 8 seconds. At that point, the contact is routed down the Error branch.

- **Response validation**: The Lambda function response could be either a STRING_MAP or JSON and has to be set while configuring the Invoke AWS Lambda function block in the flow. If response validation is set to STRING_MAP, then the lambda function should return a flat object of key/value pairs of the string type. Otherwise, if response validation is set to JSON, the lambda function can return any valid JSON including nested JSON.
Configuration tips

- To use an AWS Lambda function in a flow, first add the function to your instance. For more information, see Add a Lambda function to your Amazon Connect instance.
- After you add the function to your instance, you can select the function from the Select a function drop-down list in the block to use it in the flow.

Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: Success and Error.

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

Sample Lambda integration

Scenarios

See these topics for scenarios that use this block:

- Invoke AWS Lambda functions

Flow block: Invoke module

Description

Calls a published module, which enables you create reusable sections of a contact flow.

For more information, see Flow modules for reusable functions.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow

Properties

The following image shows the Properties page of the Invoke module block.

Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: Success and Error.
Flow block: Loop

Description

- Counts the number of times customers are looped through the Looping branch.
- After the loops are completed, the Complete branch is followed.
- This block is often used with a Get customer input block. For example, if the customer doesn't succeed in entering their account number, you can loop to give them another opportunity to enter it.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- All flows
Properties

The following image shows the Properties page of the Loop block. It is configured to repeat three times, and then it branches.

Configuration tips

• If you enter 0 for the loop count, the Complete branch is followed the first time this block runs.

Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: Looping and Complete.

Flow block: Loop prompts

Description

• Loops a sequence of prompts while a customer or agent is on hold or in queue.
**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Customer Queue flow
- Customer Hold flow
- Agent Hold flow

**Properties**

The following image shows the Properties page of the Loop prompts block. It shows there are three types of prompts you can choose from the dropdown list: Audio recording, Text to Speech, S3 file path.
How the Interrupt option works

Let's say you have multiple prompts and you set **Interrupt** to 60 seconds. Following is what will happen:

- The block plays prompts in the order that they are listed for the entirety of the prompt length.
- If the combined play time for the prompts is 75 seconds, after 60 seconds the prompt is interrupted and reset to the 0 second point again.
- It's possible your customers would never hear potentially important information that is supposed to play after 60 seconds.

This scenario is especially possible when using the default audio prompts that Amazon Connect provides since these audio prompts can be as long as 4 minutes.

**Configuration tips**

- The following blocks are not allowed before the **Loop prompts** block:
  - Get customer input
  - Loop
  - Play prompt
  - Start media streaming
  - Stop media streaming
- Store customer input
- Transfer to phone number
- Transfer to queue, including Transfer to callback queue

For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the Play prompt block.

When Loop prompts is used in a Queue flow, audio playback can be interrupted with a flow at preset times.

Always use an interruption period that's greater than 20 seconds. This is the amount of time an available agent has to accept the contact. If the interruption period is less than 20 seconds, you might get contacts going down the Error branch. This is because Amazon Connect doesn't support dequeuing the customer when they are being routed to an active agent and are in the 20 second window to join.

The internal counter for the loop is persisted for the call, not the flow. If you reuse the flow during a call, the loop counter isn't reset.

If this block is triggered during a chat conversation, the contact is routed down the Error branch.

Some existing flows have a version of the Loop prompts block that doesn't have an Error branch. In this case, a chat contact stops execution of the customer queue flow. The chat is routed when the next agent becomes available.

**Configured block**

The following image shows what this block looks like when it is configured to play a prompt from the Amazon Connect library. Choose + next to Audio Recording to view the full name of the file. The configured block has two branches: Timeout and Error.

The following image shows what this block looks like when it is configured to play a prompt from Amazon S3. Choose + next to S3 path to view the full path. The configured block has two branches: Timeout and Error.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample interruptible queue flow with callback

Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue

Flow block: Play prompt

Description

- This block can play an audio prompt, play a text-to-speech message, or send a chat response.
- Amazon Connect includes a set of pre-recorded prompts for you to use.
- To use your own voice prompts, you have the following options:
  - **Use the Amazon Connect library**: You can record and upload your audio prompts in using the Amazon Connect admin website. For instructions, see Create prompts.
  - **Use Amazon S3**: You can store as many voice prompts as needed in Amazon S3 and access them in real time by using contact attributes in the Play prompt block.

For example, based on a customer's preferred language, you can dynamically play a voice prompt with a local accent that greets them and thanks them for being a loyal member. You can even concatenate multiple attributes, such as line of business or language preference to create personalized interactions; for example, reservations + Spanish language.
Requirements

- **Supported formats:** Amazon Connect supports .wav files to use for your prompt. You must use .wav files that are 8KHz, and mono channel audio with U-Law encoding. Otherwise, the prompt won't play correctly. You can use publicly available third-party tools to convert your .wav files to U-Law encoding. After converting the files, upload them to Amazon Connect.

- **Size:** Amazon Connect supports prompts that are less than 50MB and less than five minutes long.

- **When storing prompts in an S3 bucket:** For Regions that are disabled by default (also called opt-in Regions) such as Africa (Cape Town), your bucket must be in the same Region.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>No - takes the <strong>Okay</strong> branch but it has no effect</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following **flow types:**

- Inbound flow
- Customer Queue flow
- Customer Whisper flow. You can play prompts from the Amazon Connect library but not prompts stored in Amazon S3.
- Agent Whisper flow: You can play prompts from the Amazon Connect library but not prompts stored in Amazon S3.
- Transfer to Agent flow
• Transfer to Queue flow

Properties

The properties provide you different ways to choose the prompt to be played.

Prompts stored in library

**Select from the prompt library (audio):** Choose from one of the pre-recorded prompts included with Amazon Connect, or use the Amazon Connect admin website to record and upload your own prompt. There's no way to upload prompts in bulk.

The following image shows the Properties page of the **Play prompt** block configured to play an Audio prompt from the prompt library.

Prompts stored in Amazon S3

**Specify an audio file from an S3 bucket:** Store as many prompts as you need in an S3 bucket and then refer to them by specifying the bucket path. For best performance, we recommend creating the S3 bucket in the same Region as your Amazon Connect instance.

The following image shows the Properties page of the **Play prompt** block configured to set the S3 file path manually.
The following image shows how to specify the S3 bucket path using attributes:

You can provide the S3 path with concatenation, as shown in the following example. This enables you to personalize the prompt, for example, by line of business and language.

Note that only the last part of path is shown in the image but you would enter the full path, for example:

https://example.s3.amazon.aws.com/"['Attributes']['Language']/"['Attributes']['LOB']"/1.wav
The following example shows how you can specify the S3 path dynamically using a user-defined attribute named **S3filepath**.

![Image of prompt selection options](image)

**Text-to-speech or chat text**

You can enter a prompt in plain text, or SSML, as shown in the following image:

![Image of text-to-speech or chat text options](image)

SSML-enhanced input text gives you more control over how Amazon Connect generates speech from the text you provide. You can customize and control aspects of speech such as pronunciation, volume, and speed.

For a list of SSML tags you can use with Amazon Connect, see [SSML tags supported by Amazon Connect](#).
For more information, see Add text-to-speech to prompts.

**Configuration tips**

- For step-by-step instructions about how to set up a dynamic prompt using contact attributes, see Dynamically select which prompts to play.

- When playing prompts from an S3 bucket, for best performance we recommend creating the bucket in the same Region as your Amazon Connect instance.

- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters, which is 6,000 characters total. You can also specify text in a flow using a contact attribute.

- Some existing flows have a version of the Play prompt block that doesn't have an Error branch. In this case, the Okay branch will always be taken at runtime. If you update the configuration of a Play prompt block that doesn't have an Error branch, an Error branch will be added to the block automatically in the editor.

- A contact is routed down the Error branch in the following situations:
  - Amazon Connect is unable to download the prompt from S3. This may be due to an incorrect file path, or the S3 bucket policy is not set up correctly and Amazon Connect does not have access. For instructions about how to apply the policy, and a template you can use, see Set up prompts to play from an S3 bucket.
  - Incorrect audio file format. Only .wav files are supported.
  - The audio file is larger than 50MB or longer than five minutes.
  - The SSML is incorrect.
  - The text-to-speech length exceeds 6000 characters.
  - The the Amazon Resource Name (ARN) for the prompt is incorrect.

**Configured block**

The following image shows what a Play prompt block looks like when it's configured for text-to-speech. It shows the text to be played, and it has two branches: Success and Error.
The following image shows what this block looks like when it's configured for an S3 bucket. It shows the S3 path, and it has two branches: **Success** and **Error**.

**Sample flows**

All of the sample flows use the **Play prompt** block. Take a look at the [Sample inbound flow (first contact experience)](#) to see a **Play prompt** for chat and one for audio.

**More resources**

See the following topics to learn more about prompts.

- [Create prompts](#)

- [Prompt actions](#) in the Amazon Connect API Reference Guide.

**Flow block: Set callback number**

**Description**

- Specify the attribute to set the callback number.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Set callback number block.
Configuration tips

- The Store customer input block often comes before this block. It stores the customer’s callback number.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success, Invalid number, and Not dialable.

1. Invalid number: The customer entered phone number that is not valid.

2. Not dialable: Amazon Connect is unable to dial that number. For example, if your instance is not allowed to make calls to +447 prefix phone numbers, and the customer requested callback to a +447 prefix number. Even though number is valid, Amazon Connect cannot call it.

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample queue configurations
- Sample queued callback: this sample only applies to previous instances of Amazon Connect.

Scenarios

See these topics for scenarios that use this block:
Flow block: Set contact attributes

Description

Stores key-value pairs as contact attributes. You set a value that is later referenced in a flow.

For example, create a personalized greeting for customers routed to a queue based on the type of customer account. You could also define an attribute for a company name or line of business to include in the text to speech strings said to a customer.

The Set contact attributes block is useful, for example, for copying attributes retrieved from external sources to user-defined attributes.

For more information about contact attributes, see Use Amazon Connect contact attributes.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- All flows
Properties

The following image shows the Properties page of the Set contact attributes block. It is configured to set a user-defined attribute on the Current contact with the key greetingPlayed and the value true.

You can choose to set attributes on:

- **Current contact**: The attributes are set on the contact that this flow is running on. The attributes are accessible by other areas of Amazon Connect, such as other flows, modules, Lambdas, contact records, and the GetMetricDataV2 API.

- **Related contact**: The attributes are associated with a new contact that contains a copy of the original contact properties.

  In the contact record, this is the RelatedContactId.

- **Flow**: The attributes are restricted to the flow in which they are configured.

  Flow attributes are useful in situations where you don't want to persist the data throughout the contact, such as when you need to use sensitive information like the customer's credit card number to do a Lambda data dip.
Flow attributes are temporary variables stored locally and only used in the flow. They aren't visible anywhere outside the flow, not even when the contact is transferred to another flow.

They can be up to 32KB (the maximum size of the contact record attributes section).

They aren't passed to a Lambda unless they are explicitly configured as parameters: in the Invoke AWS Lambda function block, choose Add a parameter.

They aren't passed to modules. You can set a flow attribute within a module, but it won't be passed out of the module.

They don't appear in the contact record.

They don't appear to the agent in the CCP.

The GetContactAttributes API can't expose them.

If you have logging enabled on the flow, the key and value appear in the Cloudwatch log.

How to reference attributes

For the JSON syntax for each attribute, see List of available contact attributes and their JSONPath reference.

To reference attributes that contain special characters in their name, such as spaces, place brackets and single quotations around the attribute name. For example: $.Attributes.

To reference attributes in the same namespace, such as a system attribute, you use the attribute name, or the name you specified as the Destination key.

To reference values in a different namespace, such as referencing an external attribute, you specify the JSONPath syntax to the attribute.

To use contact attributes to access other resources, set a user-defined attribute in your flow and use the Amazon Resource Name (ARN) of the resource you want to access as the value for the attribute.

Lambda examples

To reference a customer name from a Lambda function lookup, use $.External.AttributeKey, replacing AttributeKey with the key (or name) of the attribute returned from the Lambda function.

To use an Amazon Connect prompt in a Lambda function, set a user-defined attribute to the ARN for the prompt, and then access that attribute from the Lambda function.
Amazon Lex examples

- To reference an attribute from an Amazon Lex bot, you use the format $.Lex. and then include the part of the Amazon Lex bot to reference, such as $.Lex.IntentName.

- To reference the customer input to an Amazon Lex bot slot, use $.Lex.Slots.slotName, replacing slotName with the name of the slot in the bot.

Configuration tips

- When using a user-defined destination key, you can name it anything you want but don’t include the $ and . (period) characters. They are not allowed because they are both used in defining the attribute paths in JSONPath.

- You can use the Set contact attribute block to set the language attribute required for an Amazon Lex V2 bot. (Your language attribute in Amazon Connect must match the language model used to build your Amazon Lex V2 bot.) The following image shows a language attribute set to Spanish.

Or, you can use the Set voice block to set the language required for an Amazon Lex V2 bot.

For more information about how to use contact attributes, see Use Amazon Connect contact attributes.

Configured block

The following image shows an example of what this block looks like when it is configured. It has two branches: Success and Error.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample inbound flow (first contact experience)

Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes

Flow block: Set customer queue flow

Description

- Specifies the flow to invoke when a customer is transferred to a queue.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Flow types

You can use this block in the following flow types:

- Inbound flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The following image shows the Properties page of the Set customer queue flow block.

For information about using attributes, see Use Amazon Connect contact attributes.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample queued callback

Flow block: Set disconnect flow

Description

- Specifies which flow to run after a disconnect event during a contact.

  A disconnect event is when:
  
  - A chat, or task is disconnected.
  
  - A task is disconnected as a result of a flow action.
  
  - A task expires. The task is automatically disconnected if it is not completed in 7 days.

  When the disconnect event occurs, the corresponding flow runs.

- Here are examples of when you might use this block:

  - Run post-contact surveys. For example, the agent asks the customer to remain on the line for a post-call survey. The agent hangs up and a disconnect flow is run. In the disconnect flow, the customer is asked a set of questions using the Get customer input block. Their answers are uploaded using an Invoke AWS Lambda function block to an external customer feedback database. The customer is thanked and disconnected.

    For more information about creating post-contact surveys, see this blog: Easily create and visualize post chat surveys with Amazon Connect and Amazon Lex. And check out this workshop: Building a contact survey solution for Amazon Connect.

  - In a chat scenario, if a customer stops responding to the chat, use this block to decide whether to run the disconnect flow and call a Wait block, or end the conversation.

  - In task scenarios where a task may not be completed in 7 days, use this block to run a disconnect flow to determine whether the task should be requeued, or completed/disconnected by a flow action.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- All flows

Properties

The following image shows the Properties page of the Set disconnect flow block.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- Sample inbound flow (first contact experience)

Scenarios

See these topics for scenarios that use this block:

- Example chat scenario
- Easily create and visualize post chat surveys with Amazon Connect and Amazon Lex
- Building a contact survey solution for Amazon Connect

Flow block: Set event flow

Description

- Specifies which flow to run during a contact event.
- The following events are supported:
  - **Default flow for agent UI**: specifies the flow to be invoked when a contact comes into the Agent Workspace. You can use this event to set up a [step-by-step](#) guide to be played to the agent in this scenario.
  - **Disconnect flow for agent UI**: specifies the flow to be invoked when a contact that is open in the Agent Workspace ends. You can use this event to set up a [step-by-step](#) guide to be played to the agent in this scenario.
**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- All flows

**Properties**

The following image shows the Properties page of the Set event flow block.
Set event flow

Specify a flow to run when a contact event or interaction occurs, such as an agent accepting or disconnecting from a call or placing a customer on hold Info

Select event

Select an event hook

Default flow for Agent UI

Select a flow

Set manually

Select a flow

This field cannot be empty.

Set dynamically
Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: **Success** and **Error**.

![Set event flow block](image)

Scenarios

See these topics for scenarios that use this block:

- [How to invoke a guide at the start of a contact](#)

Flow block: Set hold flow

Description

- Links from one flow type to another.
- Specifies the flow to invoke when a customer or agent is put on hold.

  If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Channel</td>
<td>Supported?</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following **flow types**:

- Inbound flow
- Customer Queue flow
- Outbound whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

The following image shows the **Properties** page of the **Set hold flow** block. It shows the dropdown list of namespaces that you can use to set the hold flow dynamically.

For information about using attributes, see [Use Amazon Connect contact attributes](#).
Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.

![Configured block diagram]

Flow block: Set logging behavior

Description

- Enables flow logs so you can track events as contacts interact with flows.
- Flow logs are stored in Amazon CloudWatch. For more information, see Flow logs stored in an Amazon CloudWatch log group.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- All flows
Properties

The following image shows the Properties page of the Set logging behavior block. It has two options: enable logging behavior, or disable it.

![Properties page](image)

Scenarios

See these topics for more information about flow logs:

- [Track events as customers interact with flows](#)

Flow block: Set recording and analytics behavior

Description

- Sets options for recording and/or monitoring (listen-in) voice and chat conversations.
- It enables features in Contact Lens. For more information, see [Analyze conversations using conversational analytics](#).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Channel</td>
<td>Supported?</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Outbound whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

The following image shows the Properties page of the Set recording and analytics behavior block. It has two sections:

- Call recording: use this section to enable or disable call recording fro the agent customer, or both.
- Analytics: use this section to enable Contact Lens analytics.
When configuring this block to set up recording behavior, choose as follows:

- To record voice conversations, choose what you want to record: **Agent and Customer**, **Agent only**, or **Customer only**.
- To record chat conversations, you need to choose **Agent and Customer**.
- To enable monitoring of voice and/or chat conversations, you need to choose **Agent and Customer**.

For information about using this block to enable Contact Lens, including features such as sensitive data redaction, see **Enable Amazon Connect Contact Lens**.

**Configuration tips**

- You can change call recording behavior in a flow, for example, change from "Agent and customer" to "Agent only." Perform the following steps:
  1. Add a second **Set recording and analytics behavior** block to the flow.
  2. Configure the second block to set call recording to **Off**.
  3. Add another **Set recording and analytics behavior** block.
4. Configure the third block to the new recording behavior you want, such as Agent only.

**Note**

The settings in the Analytics section are overwritten by each subsequent Set recording and analytics behavior block in the flow.

- **For calls:** Unchecking Enable Contact Lens conversational analytics disables Contact Lens analytics.

  For example, let's say you have two Set recording and analytics behavior blocks in your flow. The first block has Enable Contact Lens conversational analytics selected. The second block later in the flow has it unselected. The analytics appear only during the time analytics was enabled.

- **For chat:** Real-time chat starts analysis as soon as any block in the flow enables it. No block later in the flow disables the real time chat settings.

- If an agent puts a customer on hold, the agent is still recorded, but the customer is not.

- If you want to transfer a contact to another agent or queue, and you want to continue using Contact Lens to collect data, you need to add to the flow another Set recording behavior block with Enable analytics turn on. This is because a transfer generates a second contact ID and contact record. Contact Lens needs to run on that contact record as well.

- When you enable Contact Lens, the type of flow that the block is in, and where it is placed in the flow, determine whether agents receive the key highlights transcript, and when they receive it.

  For more information and example use cases that explain how the block affects the agents experience with key highlights, see Design a flow for key highlights.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It has one branch: **Success**.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample inbound flow (first contact experience)

Scenarios

See these topics for scenarios that use this block:

- Set up recording behavior
- Set up live monitoring for voice and/or chat
- Review recorded conversations between agents and customers using Amazon Connect
- Analyze conversations using conversational analytics

Flow block: Set Voice ID

Description

- Enables audio streaming and sets thresholds for voice authentication and detection of fraudsters in a watchlist. For more information about this feature, see Voice ID.
- Sends audio to Amazon Connect Voice ID to verify the caller's identity and match against fraudsters in watchlist, as soon as the call is connected to a flow.
• Use a **Play prompt** block before **Set Voice ID** to stream audio properly. You can edit it to include a simple message such as "Welcome."

• Use a **Set contact attributes** block after **Set Voice ID** to set the customer ID for the caller.

  The `CustomerId` may be a customer number from your CRM, for example. You can create a Lambda function to pull the unique customer ID of the caller from your CRM system. Voice ID uses this attribute as the `CustomerSpeakerId` for the caller.

  `CustomerId` can be an alphanumeric value. It supports only _ and - (underscore and hyphen) special characters. It does not need to be UUID. For more information, see `CustomerSpeakerId` in the **Speaker** data type.

• Use a **Check Voice ID** block after **Set Voice ID** to branch based on the results of the enrollment check, authentication, or fraud detection.

• For information about how to use **Set Voice ID** in a flow, along with **Check Voice ID** and **Set contact attributes**, see Step 2: Create a new Voice ID domain and encryption key in **Enable Voice ID**.

### Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

### Flow types

You can use this block in the following **flow types**:

• Inbound flow

• Customer queue flow

• Customer whisper flow
• Outbound whisper flow
• Agent whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the Set Voice ID block. It shows the Voice authentication section. In this example, the Authentication Threshold is set to 90. This is the recommended threshold.

Start streaming audio for Voice ID

When this option is selected, Amazon Connect begins streaming audio from the customer's channel to Voice ID.

You can add this block several places in a flow, but after Start streaming audio is selected, it cannot be disabled, even if later in the flow there are other Set Voice ID blocks that do not have it enabled.

Voice authentication

Authentication threshold: When Voice ID compares the voiceprint of the caller to the enrolled voiceprint of the claimed identity, it generates an authentication score between 0-100. This score
indicates the confidence of a match. You can configure a threshold for the score which indicates whether the caller is authenticated. The default threshold of 90 provides high security for most cases.

- If the authentication score is below the configured threshold, Voice ID treats the call as not authenticated.
- If the authentication score is above the configured threshold, Voice ID treats the call as authenticated.

For example, if the person is sick and calling from a mobile device in their car, the authentication score is going to be slightly lower than when the person is well and calling from a quiet room. If an imposter is calling, the authentication score is much lower.

**Authentication response time**

You can set the authentication response time between 5 and 10 seconds, which determines how quickly you want Voice ID authentication analysis to complete. Lowering it makes the response time faster at the tradeoff of lower accuracy. When you're using self-service IVR options where callers do not talk a lot, you may want to reduce this time. You can then increase the time if the call needs to be transferred to an agent.

The following image shows the Authentication Response time section of the block. The response time is set manually to 10 seconds.

![Authentication Response time](image)

Choose **Set dynamically** to set the authentication threshold based on certain criteria. For example, you may want to raise the threshold based on the membership level of the customer, or the type of transaction or information they are calling about.
Fraud detection

The threshold you set for fraud detection is used to measure risk. Scores higher than the threshold are reported as higher risk. Scores lower than the threshold are reported as lower risk. Raising the threshold lowers false positive rates (makes result more certain), but raises false negative rates.

Choose Set dynamically to set the fraud threshold based on certain criteria. For example, you may want to lower the threshold for high wealth customers, or the type of transaction or information they are calling about.

The watchlist you select is used when evaluating the voice session. Choose Use default watchlist to use your domain's default watchlist. For Set manually, the watchlist ID must be 22 alphanumeric characters.

Similarly for the watchlist, choose Set dynamically to set the watchlist based on criteria given. For example, you may want to use a stricter watchlist given the type of transaction or information they are calling about.

Configuration tips

- For the Authentication threshold, we recommend that you start with the default of 90 and adjust until you find a good balance for your business.

  Every time you increase the value of the Authentication threshold beyond the default of 90, there's a tradeoff:
• The higher the threshold, the greater the false reject rate (FRR), that is, the likelihood that an agent will need to verify the customer's identity.

  For example, if you set it too high, such as greater than 95, agents will need to verify every customer's identity.

• The lower the threshold, the greater the false acceptance rate (FAR), that is, the likelihood that Voice ID will incorrectly accept an access attempt by an unauthorized caller.

• When Voice ID verifies that the voice belongs to the enrolled customer, it returns a status of Authenticated. Add a Check Voice ID block to your flow branch based on the returned status.

• For the Fraud threshold, we recommend that you start with the default of 50 and adjust until you find a good balance for your business.

  If the caller's score is above the threshold, it indicates there's a higher risk for fraud in that call.

• For the Fraud watchlist, the format is validated when the flow is published.
  - If a watchlist is dynamically set and the format is not valid, the contact is routed down the Error branch of the Set Voice ID block.
  - If a watchlist ID is set manually or dynamically with a valid format but the watchlist is not available in the Voice ID domain of the instance, the contact is routed down the Error branch of Check Voice ID block when the Check Voice ID block is used later in the flow.

**Configured block**

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.

![Configured block image](image-url)

**More information**

See the following topic for more information about this block:

- Use real-time caller authentication with Voice ID
- Flow block: Check Voice ID
Flow block: Set voice

Description

• Sets the text-to-speech (TTS) language and voice to use for the contact flow.
• The default voice is configured to Joanna (Conversational speaking style).
• You can choose Override speaking style to make it and other voices Amazon Polly Neural Text-to-Speech (NTTS). Neural voices make automated conversations sound more lifelike by improving the pitch, inflection, intonation, and tempo.

For a list of supported neural voices, see Neural Voices in the Amazon Polly Developer Guide.
• After this block is run, any TTS invocation resolves to the neural or standard voice selected.
• If this block is triggered during a chat conversation, the contact goes down the Success branch. It has no effect on the chat experience.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Success branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Success branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

• All flows
Properties

The following image shows the Properties page of the Set voice block. It is configured for English, the voice is Joanna, and the speech style is Conversational.

Tip

For voices that support only neural speaking styles but not standard, the Override speaking style is automatically selected. You do not have the option to clear it.

Use an Amazon Lex V2 bot with Amazon Connect

If you're using an Amazon Lex V2 bot, your language attribute in Amazon Connect must match the language model used to build your Lex bot. This is different than Amazon Lex (Classic).

• If you build an Amazon Lex V2 bot with a different language model—for example, en_AU, fr_FR, es_ES, and more—under Voice, choose a voice that corresponds to that language, and then must choose Set language attribute, as shown in the following image.

• If you're not using an en-US voice with an Amazon Lex V2 bot and don't choose Set language attribute, the Get customer input block results in an error.

• For bots with multiple languages (for example, en_AU and en_GB) choose Set language attribute for one of the languages, as shown in the following image.
Configuration tips

- For the Joanna and Matthew neural voices, in American English (en-US), you can also specify a Conversational speaking style or a Newscaster speaking style.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branch: Success.

Scenarios

See these topics for scenarios that use this block:

- Add text-to-speech to prompts
Flow block: Set whisper flow

Description

A whisper flow is what a customer or agent experiences when they are joined in a voice or chat conversation. For example:

- An agent and customer are joined in a chat. An agent whisper might display text to the agent telling them the name of the customer, for example, which queue the customer was in, or let the agent know they're talking to club member.
- An agent and customer are joined in a call. A customer whisper might tell the customer that the call is being recorded for training purposes, for example, or thank them for being a club member.
- An agent and customer are joined in a chat. Using a contact attribute, an agent whisper flow records which agent is being connected to the conversation. This attribute is then used in a disconnect flow to route the contact back to the same agent if the customer has a follow-up question after the agent disconnects.

A whisper flow has the following characteristics:

- It's a one-sided interaction: either the customer hears or sees it, or the agent does.
- It can be used to create personalized and automated interactions.
- It runs when a customer and agent are being connected.

For voice conversations, the Set whisper flow block overrides the default agent whisper flow or customer whisper flow by linking to a whisper flow you create.

⚠️ Important

For chat conversations, you need to include a Set whisper flow block for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation.

How the Set whisper flow block works

- For inbound conversations (voice or chat), the Set whisper flow block specifies the whisper to be played to customer or the agent when they are joined.
• For outbound voice calls, it specifies the whisper to be played to customer.

• A whisper is one direction, which means only the agent or customer hears or sees it, depending on the type of whisper you selected. For example, if a customer whisper says "This call is being recorded," the agent does not hear it.

• A whisper flow is triggered after the agent accepts the contact (either auto-accept or manual accept). The agent whisper flow runs first, before the customer is taken out of queue. After this is completed, the customer is taken out of queue and the customer whisper flow runs. Both flows run to completion before the agent and customer can talk or chat with each other.

• If an agent disconnects while the agent whisper is running, the customer remains in queue in order to be re-routed to another agent.

• If a customer disconnects while the customer whisper is running, the contact ends.

• If an agent whisper flow or customer whisper flow includes a block that chat does not support, such as Start/Stop media streaming or Set voice, chat skips these blocks and triggers an error branch. However, it doesn't prevent the flow from progressing.

• Whisper flows don't appear in transcripts.

• Whispers can be a maximum of 2 minutes long. After that point, the contact or agent is disconnected.

**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

• Inbound flow

• Customer Queue flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the Set whisper flow block. It shows the whisper to the agent is set manually to Default agent whisper. Use the dropdown box to choose a different whisper flow.

If you choose to Select a flow, you can only select from flows that are type Agent Whisper or Customer Whisper.

For information about using attributes, see Use Amazon Connect contact attributes.

Configuration tips

• In a single block, you can set either a customer whisper or an agent whisper, but not both. Instead, use multiple Set whisper flow blocks in your flow.

• If you use a Play prompt block instead of a Set whisper block in an agent whisper flow or customer whisper flow, in a voice conversation the prompt is audible to both the agent and the customer. In a chat, however, only the agent or customer sees the Play prompt text.

• Make sure your whispers are able to complete within two minutes. Otherwise, calls will be disconnected before being established.

• If agents appear to be stuck in the "Connecting..." state before being forcefully disconnected from calls, make sure that your configured whisper flows meet the two minute maximum.
Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: **Success** and **Error**.

![Set working queue block diagram](image)

Flow block: Set working queue

Description

- This block specifies the queue to be used when **Transfer to queue** is invoked.
- A queue must be specified before invoking **Transfer to queue** except when used in a customer queue flow. It's also the default queue for checking attributes, such as staffing, queue status, and hours of operation.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following **flow types**:

- Inbound flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following image shows the Properties page of the Set working queue block. It is set to the BasicQueue.

Note the following properties:

• By queue > Set dynamically. To set the queue dynamically, you must specify the Amazon Resource Name (ARN) for the queue rather than the queue name. To find the ARN for a queue, open the queue in the queue editor. The ARN is included as the last part of the URL displayed in the browser address bar after /queue. For example, aaaaaaaaa-bbbb-cccc-dddd-111111111111.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample queue customer
- Sample queue configurations

Scenarios

See these topics for scenarios that use this block:

- Set up agent-to-agent transfers
- Transfer contacts to a specific agent

Flow block: Show view

Description

- Use this block configure UI-based workflows that you can surface to users of front end applications. You can use this block to create step-by-step guides for agents who are using the Amazon Connect agent workspace.
- To use this block, first select a View resource from a drop-down menu and then map data to the different fields in the View's schema. You can use the Set JSON mapping option which lets you pass in entire JSON objects. For details on the available View templates, see View resource.
- When the block receives a response back from the client application, the output data can be referenced in flows using $.Views.ViewResultData.
• Check out our library of samples and reusable modules to help you get started with using the Show view block and creating step-by-step guides. These modules show how you can configure the different types of Show view blocks and ways you can integrate step-by-step guides with other workflows and services. They demonstrate good design patterns for common and complex use cases, and address the most common design concerns.

To load the samples into your Amazon Connect instance, use the Import/export flows feature to load the flow with the sample Show view block into your account.

Supported channels

This block routes step-by-step guides that are to be displayed to agents in the agent workspace. It routes the guides as chat contacts. This type of chat contact is different from the customer-based contact that the agent is handling.

For example, a premium customer may call your contact center. The Show view block is triggered to display the premium step-by-step guide to the agent. There are two contacts involved:

• The customer, who is a voice contact.
• The step-by-step guide, which is routed as a chat contact.

Flow types

You can use this block in the following flow type:

• Inbound flow

Properties

Properties are dynamically populated depending on which View resource you select. The following image shows the Properties page of the Show view block. It is set to the Wizard solution view.
Show View

Renders a View in a user application and waits for a response from the application Info

Solution View

Select a solution view. Info

Solution View
Wizard

Steps

- Set manually

  Steps

  - Set dynamically

  - Set JSON

StepSection

- Set manually

  StepSection

  - Set dynamically

  - Set JSON

Heading

- Set manually

  Heading

  File missing luggage claim

Cancel  Save
How to use the Set JSON option

This section walks through an example of how to use the Set JSON option.

1. In the View section of the Properties page, choose Confirmation from the dropdown menu, as shown in the following image.

When you choose the Confirmation View, the input schema of the View is displayed on the properties page. The schema has the following sections where you can add information: Heading, AttributeBar, Graphic, Next, Style, Subheading, and Timeout. The following image shows some of these sections.
2. The following image shows the **AttributeBar** parameter, the **Set using JSON** option. To view all of the JSON you pasted in, click the corner of the box and pull down.
Tip

Fix any errors if the JSON is invalid. The following image shows an example error message because there's an extra comma.

![JSON example with invalid JSON](image)

3. Choose Save and publish when you are ready.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Back, Next, No Match, Error, and Timeout.

The chat contact is routed down the Back or Next branches depending on what the user clicks on the View. No match is only possible if the user has an action component with a custom Action value.
Flow block: Start media streaming

Description

Captures what the customer hears and says during a contact. You can then perform analysis on the audio streams to:

- Determine customer sentiment.
- Use the audio for training purposes.
- Identify and flag abusive callers.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.
## Channel Supported?

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

### Flow types

You can use this block in the following **flow types**:

- Inbound flow
- Customer Queue flow
- Customer Whisper flow
- Outbound Whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

### Properties

The following image shows the **Properties** page of the **Start media streaming** block. It has two options: start the stream from the customer or to the customer.

![Start media streaming](image)

- Starts streaming media to Kinesis. [Learn more](#)
- Only audio is supported

**Select stream to start**

- [ ] From the customer
- [x] To the customer
Configuration tips

• You must enable live media streaming in your instance to successfully capture customer audio. For instructions, see Set up live media streaming of customer audio.

• Customer audio is captured until a Stop media streaming block is invoked, even if the contact is passed to another flow.

• You must use a Stop media streaming block to stop media streaming.

• If this block is triggered during a chat conversation, the contact is routed down the Error branch.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.

![Configured block image]

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

Example flow for testing live media streaming

Flow block: Stop media streaming

Description

• Stops capturing customer audio after it is started with a Start media streaming block.

• You must use a Stop media streaming block to stop media streaming.
Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Customer Whisper flow
- Outbound Whisper flow
- Agent Whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

This block doesn't have any properties.

Configuration tips

- You must enable live media streaming in your instance to successfully capture customer audio. For instructions, see Set up live media streaming of customer audio.
- Customer audio is captured until a Stop media streaming block is invoked, even if the contact is passed to another flow.
- If this block is triggered during a chat conversation, the contact is routed down the Error branch.
Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success and Error.

![Image showing configured block]

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

Example flow for testing live media streaming

Flow block: Store customer input

Description

This block is similar to Get customer input, but this one stores the input as a contact attribute (in the Stored customer input system attribute) and allows you to encrypt it. This way, you can encrypt sensitive input such as credit card numbers. This block:

- Plays a prompt to get a response from the customer. For example, "Please enter your credit card number" or "Please enter the phone number we should use to call you back."
- Plays an interruptible audio prompt or play text-to-speech for a customer to respond to.
- Stores numerical input as in the Stored customer input system attribute.
- Allows you to specify a custom terminating keypress.
- If during a call the customer doesn't enter any input, the contact is routed down the Success branch branch with a value of Timeout. Add a Check contact attributes block to check for timeouts.
**Supported channels**

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

**Flow types**

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

The following image shows the Properties page of the Store customer input block. It shows the Prompt section configured to play the Audio prompt.
The following image shows the **Customer input** section of the page. It is configured to allow up to 20 digits. It is set to timeout after 5 seconds of no input.

Note the following properties:

- For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the **Play prompt** block.
- **Maximum Digits**: Define the maximum number of digits that a customer can enter.
- **Timeout before first entry**: Specify how long to wait for a customer to start entering their reply by voice or DTMF. For example, you might enter 20 seconds, to give the customer time to get their credit card.
After the contact starts entering digits, Amazon Connect waits 5 seconds for each digit, by default. You cannot change this default setting.

- **Encrypt entry**: Encrypt the customer's entry, such as their credit card information. For step-by-step instructions to get the keys that you use to input this information, see [Creating a secure IVR solution with Amazon Connect](#).

- **Specify terminating keypress**: Define a custom terminating keypress that is used when your contacts complete their DTMF inputs. The terminating keypress can be up to five digits long, with #, *, and 0-9 characters, instead of just #.

  - **Note**: To use a star (*) as part of the terminating keypress, you must also choose **Disable cancel key**.

- **Disable cancel key**: By default, when a customer enters * as input, it deletes all of the DTMF input that came before it. However, if you choose **Disable cancel key**, Amazon Connect treats the * as any other key.

  If you send the DMTF input to an **Invoke AWS Lambda function** block, the **Disable cancel key** property affects the input, as follows:

  - When **Disable cancel key** is selected, all the characters entered—including any *—are sent to the **Invoke Lambda function** block.
  - When **Disable cancel key** is not selected, only the * is sent to the **Invoke Lambda function** block.

  For example, let's say you chose **Disable cancel key**, and a customer entered 1#2#3*4###, where ## is the terminating keypress. The **Invoke Lambda function** block then receives the entire 1#2#3*4# as input. You could program the Lambda function to ignore the character before the * character. So, the customer input would be interpreted as 1#2#4#.

- **Phone number**: This option is useful for queued callback scenarios.

  - **Local format**: If all of your customers all calling from the same country that your instance is in, choose that country from the dropdown list. Amazon Connect then auto-populates the country code for customers so that they don't have to enter it.

  - **International format**: If you have customers calling from different countries, choose **International format**. Amazon Connect then requires customers to enter their country code.
Problems with DTMF input?

Let's say you have the following scenario with two contacts flows, each one capturing DTMF input from customers:

1. One flow uses the Get customer input block to request DTMF input from customers.
2. After the DTMF input is entered, it uses the Transfer to flow block to move the contact to the next contact flow.
3. In the next flow, there's a Store customer input block to get more DTMF input from the customer.

There's setup time between the first and second flows. This means if the customer enters DTMF input very quickly for the second flow, some of the DTMF digits might be dropped.

For example, the customer needs to press 5, then wait for a prompt from the second flow, then type 123. In this case, 123 is captured without problem. However, if they don't wait for the prompt and enter 5123 very quickly, the Store customer input block may capture only 23 or 3.

To guarantee the Store customer input block in second contact flow captures all of the digits, the customer needs to wait for the prompt to be played, and then enter their type DTMF input.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branches: Success, Error, and Invalid number.

1. **Invalid number**: What to do if the customer enters an invalid number.
Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample secure input with agent
- Sample secure input with no agent
- Sample queue configurations
- Sample queued callback

Scenarios

Creating a secure IVR solution with Amazon Connect

Flow block: Transfer to agent (beta)

Description

- Ends the current flow and transfers the customer to an agent.

⚠️ Note

If the agent is already with someone else, the contact is disconnected.
If the agent is in After Contact Work, they are automatically removed from ACW at the time of transfer.

- The Transfer to Agent block is a beta feature and works only for voice interactions.
- We recommend using the Set working queue block for agent-to-agent transfers instead of using this block. The Set working queue block supports omnichannel transfers such as voice and chat. For instructions, see Set up agent-to-agent transfers.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.
<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

To transfer chats and tasks to agents, use the `Set working queue` block. Because `Set working queue` works for all channels, we recommend using it for voice calls too, instead of using `Transfer to agents (beta)`. For instructions, see [Set up agent-to-agent transfers](#).

**Flow types**

You can use this block in the following flow types:

- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

The following image shows the Properties page of the `Transfer to agent` block. It does not have any options on it.

![Properties page of Transfer to agent block](image)

**Configured block**

The following image shows an example of what this block looks like when it is configured. It displays the status `Transferred`. It does not have any branches.
Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers

Flow block: Transfer to flow

Description

- Ends the current flow and transfers the customer to a different flow.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

The following image shows the Properties page of the Transfer to flow block. You choose the flow from the dropdown box.

Only published flows appear in the dropdown list.

Configured block

The following image shows an example of what this block looks like when it is configured. It has the following branch: Error.

1. The contact is routed down the Error branch if the flow you have specified to transfer to isn't a valid flow, or it's not a valid flow type (Inbound, Transfer to Agent, or Transfer to Queue).

Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see Sample flows. Following are topics that describe the sample flows which include this block.

- Sample AB test
Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers

Flow block: Transfer to phone number

Description

- Transfers the customer to a phone number external to your instance.
- If this block is triggered during a chat conversation, the contact is routed down the Error branch.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Task</td>
<td>No - Error branch</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

The following image shows the Properties page of the Transfer to phone number block. It shows the Transfer via section. The Country code is set to +1 (US). Set timeout = 30 seconds.

The following image shows the Resume flow after disconnect section is set to Yes.

Note the following properties:
Resume flow after disconnect: This works only if the external party disconnects, and the customer doesn't disconnect. (If the customer disconnects, the whole call disconnects.)

Send DTMF: This property is useful to bypass some of the DTMF of the external party. For example, if you know you'll need to press 1, 1, 362 to reach the external party, you can enter that here.

Caller ID number: You can choose a number from your instance to appear as the caller ID. This is useful in cases where you want to use a number that's different from the one the flow is actually using to make the call.

**Important**

If you are using Amazon Connect outside of the United States, we recommend choosing Caller ID number and then selecting an Amazon Connect number. Otherwise, local regulations may cause telephony providers to block or redirect non-Amazon Connect phone numbers. This will result in service-related events, such as rejected calls, poor audio quality, delay, latency, and displaying the incorrect caller ID.

In Australia: The caller ID must be an Amazon Connect provided DID (Direct Inward Dialing) phone number. If a toll free number or a number not provided by Amazon Connect is used in the caller ID, local telephony suppliers may reject outbound calls due to local anti-fraud requirements.

In the UK: The caller ID must be a valid E164 phone number. If the phone number is not provided in the caller ID, local telephony suppliers may reject outbound calls due to local anti-fraud requirements.

Caller ID name: You can set a caller ID name, but there's no guarantee it will appear correctly to the customer. For more information, see Outbound caller ID number.

**Note**

When Transfer to phone number block is used without specifying a custom caller ID, the caller ID of the caller is passed as the caller ID. For example, if you transfer to an external number and no custom caller ID is used to specify that the call is coming from your organization, then the contact's caller ID is displayed to the external party.
Configuration tips

- **Submit a service quota increase request** requesting that your business be allowed to make outbound calls to the country you specified. If your business is not on the allowlist for making the call, it will fail. For more information, see [Countries you can call by default](#).

- If the country you want to select is not listed, you can submit a request to add countries you want to transfer calls to using the [Amazon Connect service quotas increase form](#).

- You can choose to end the flow when the call is transferred, or choose to **Resume flow after disconnect**, which returns the caller to your instance and resumes the flow after the transferred call ends.

Configured block

The following image shows an example of what this block looks like when it is configured. It shows the number you are transferring to. It has the following branches: **Success, Call Failed, Timeout, Error**.

![Configured block](#)

Scenarios

See these topics for scenarios that use this block:

- [Set up contact transfers](#)
- [Set up outbound caller ID](#)
Flow block: Transfer to queue

Description

- In most types of flows, this block ends the current flow and places the customer in a queue.
- When used in a Customer Queue flow, however, this block transfers a contact already in a queue to another queue.
- When used in a callback scenario, Amazon Connect calls the agent first. After the agent accepts the call in the CCP, Amazon Connect calls the customer.
- This block cannot be used in a callback scenario when using the chat channel. If you attempt to do so, an error is created in the CloudWatch log.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Yes</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

This block has two tabs on its properties page.
**Tab 1: Transfer to queue:** This tab is shown in the following image.

When the **Transfer to queue** block runs, it checks the queue capacity to determine whether the queue is at capacity (full). This check for queue capacity compares the current number of contacts in the queue to the [Maximum contacts in queue](#) limit, if one is set for the queue.

If no limit is set, the queue is limited to the number of concurrent contacts set in the service quota for the instance.

**Tab 2: Transfer to callback queue:** This tab is shown in the following image.
The following properties are available under the **Transfer to callback queue** tab:

- **Initial delay**: Specify how much time has to pass between a callback contact being initiated in the flow, and the customer is put in queue for the next available agent.

- **Maximum number of retries**: If this were set to 1, then Amazon Connect would try to callback the customer at most two times: the initial callback, and 1 retry.

**Tip**

We strongly recommend that you double-check the number entered in **Maximum number of retries**. If you accidentally enter a high number, such as 20, it's going to result in unnecessary work for the agent and too many calls for the customer.

- **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait until trying again.
- **Set working queue**: You can transfer a callback queue to a different queue. This is useful if you set up a special queue just for callbacks. You can then view that queue to see how many customers are waiting for callbacks.

  **Tip**

  If you want to specify the **Set working queue** property, you need to add a **Set customer callback number** block before this block.

If you don't set a working queue, Amazon Connect uses the queue that was set previously in the flow.

**Configuration tips**

- When you use this block in a Customer Queue flow, you must add a **Loop prompts** block before this one.
- To use this block in most flows, you must add a **Set working queue** block first. The one exception to this rule is when this block is used in a Customer Queue flow.
- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters (6,000 total characters).
- Amazon Lex bots support both spoken utterances and keypad input when used in a flow.
- You can prompt contacts to end their input with a pound key `#` and to cancel it using the star key `*`.

**Configured block**

When this block is configured to **transfer to queue**, it looks similar to the following image. It has two branches: **At capacity** and **Error**. If a contact is routed down the **At capacity** branch, it remains in the current working queue.
When this block is configured to **transfer to callback queue**, it looks similar to the following image. It has two branches: **Success** and **Error**. If a contact is routed down the **Success** branch, it's transferred to the specified queue.

### Scenarios

See these topics for scenarios that use this block:

- [Manage contacts in a queue](#)
- [Set up queued callback by creating flows, queues, and routing profiles](#)
- [About queued callbacks in metrics](#)

### Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- [Sample queue configurations](#)
- [Sample customer queue priority](#)
- [Sample queued callback](#)
Flow block: Wait

Description

This block pauses the flow for the specified wait time.

For example, if a contact stops responding to a chat, the block pauses the contact flow for the specified wait time (Timeout time), then branches accordingly, such as to disconnect.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>No - Error branch</td>
</tr>
<tr>
<td>Chat</td>
<td>Yes</td>
</tr>
<tr>
<td>Task</td>
<td>Yes - It always branches to Time Expired or Error. It never branches to Bot participant disconnected or Participant not found. The Participant Type setting does not affect this behavior.</td>
</tr>
</tbody>
</table>

Flow types

You can use this block in the following flow types:

- Inbound flow
- Customer Queue flow

Properties

The following image shows the Properties page of the Wait block. It is configured pause the flow for 5 hours.
It has the following properties:

- **Participant Type**: Runs the Wait block for the specified participant type.
  - **Default**: A customer contact.
  - **Bot**: A custom participant, such as a third-party bot. For more information about using this option, see [Customize chat flow experiences by integrating custom participants](#).

- **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. Maximum is 7 days.
  - Manually set timeout: You can provide the **Number** and **Units**.
  - Dynamically set timeout: The unit of measurement is in seconds.

- **Customer return**: Route the contact down this branch when the customer returns and sends a message. With this branch you can route the customer to the previous (same) agent, previous (same) queue, or override and set a new working queue or agent. This optional branch is available only when **Participant Type** = **Default**.

**Configuration tips**

You can add multiple Wait blocks to your contact flows. For example:

- If the customer comes back in 5 minutes, connect them to the same agent. This is because that agent has all of the context.

- If the customer doesn't come back after 5 minutes, send a text saying "We missed you."
• If the customer comes back in 12 hours, connect to a flow that puts them in a priority queue. However, it doesn't route them to the same agent.

**Configured block**

The following image shows an example of what this block looks like when it is configured with **Participant Type = Default**. It has the following branches: **Time Expired** and **Error**.

![Wait block with Default Participant Type](image)

The following image shows an example of what this block looks like when it is configured with **Participant Type = Bot**. It has the following branches: **Bot participant disconnected**, **Participant not found**, **Time Expired**, and **Error**.

![Wait block with Bot Participant Type](image)

1. **Bot participant disconnected**: The custom participant, such as a third-party bot, has successfully disconnected to the contact.
2. **Participant not found**: No custom participant was found to be associated to the contact.

3. **Time Expired**: The timeout specified has lapsed before the custom participant disconnected.

### Sample flows

Amazon Connect includes a set of sample flows. For instructions that explain how to access the sample flows in the flow designer, see [Sample flows](#). Following are topics that describe the sample flows which include this block.

- **Sample disconnect flow**

### Scenarios

See these topics for scenarios that use this block:

- **Example chat scenario**

### Create a flow

The starting point for creating all flows is the flow designer. It’s a drag-and-drop work surface that enables you to link together blocks of actions. For example, when a customer first enters your contact center, you can ask for some input and then play a prompt such as "Thank you."

For descriptions of the available flow blocks, see [Flow block definitions](#).

### Contents

- **Before you begin: develop a naming convention**
- **Choose a flow type**
- **Create an inbound flow**
- **Use the mini-map to navigate a flow**
- **Customize the name of a block**
- **Undo and redo actions in the flow designer**
- **Add notes to a block**
- **Copy and paste flows**
- **Archive, delete, and restore flows**
Before you begin: develop a naming convention

Chances are you're going to create tens or hundreds of flows. To help you stay organized, it's important to develop a naming convention. After you start creating flows, we strongly recommend against renaming them.

Choose a flow type

Amazon Connect includes a set of nine flow types. Each type has only those blocks for a specific scenario. For example, the flow type for transferring to a queue contains only the appropriate flow blocks for that type of flow.

**Important**

- When you create a flow, you need to choose the right type for your scenario. Otherwise, the blocks you need may not be available.
- You can't import flows of different types. This means if you start with one type and need to switch to another to get the right blocks, you have to start over.

The following flow types are available.

<table>
<thead>
<tr>
<th>Type</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound flow</td>
<td>This is the generic flow type that's created when you choose the Create flow button, and don't select a type using the drop-down arrow. It creates an inbound flow. This flow works with voice, chat, and tasks.</td>
</tr>
<tr>
<td>Customer queue flow</td>
<td>Use to manage what the customer experiences while in queue, before being joined to an...</td>
</tr>
<tr>
<td>Type</td>
<td>When to use</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Agent hold flow</strong></td>
<td>Use to manage what the customer experiences while the customer is on hold. With this flow, one or more audio prompts can be played to a customer using the Loop prompts block while waiting on hold.</td>
</tr>
<tr>
<td></td>
<td>This flow works with voice.</td>
</tr>
<tr>
<td><strong>Customer whisper flow</strong></td>
<td>Use to manage what the customer experiences as part of an inbound call immediately before being joined with an agent. The agent and customer whispers are played to completion, then the two are joined.</td>
</tr>
<tr>
<td></td>
<td>This contact flow works with voice and chat.</td>
</tr>
<tr>
<td><strong>Outbound whisper flow</strong></td>
<td>Use to manage what the customer experiences as part of an outbound call before being connected with an agent. In this flow, the customer whisper is played to completion, then the two are joined. For example, this flow can be used to enable call recordings for outbound calls with the Set recording behavior block.</td>
</tr>
<tr>
<td></td>
<td>This contact flow works with voice and chat.</td>
</tr>
<tr>
<td>Type</td>
<td>When to use</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent hold flow</td>
<td>Use to manage what the agent experiences when on hold with a customer. With this flow, one or more audio prompts can be played to an agent using the Loop prompts block while the customer is on hold. This flow works with voice.</td>
</tr>
<tr>
<td>Agent whisper flow</td>
<td>Use to manage what the agent experiences as part of an inbound call immediately before being joined with a customer. The agent and customer whispers are played to completion, then the two are joined. This contact flow works with voice, chat, and tasks.</td>
</tr>
<tr>
<td>Type</td>
<td>When to use</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Transfer to agent flow</strong></td>
<td>Use to manage what the agent experiences when transferring to another agent. This type of flow is associated with transfer to agent quick connects, and often plays messaging, then completes the transfer using the <strong>Transfer to agent</strong> block. This flow works with voice, chat, and tasks.</td>
</tr>
<tr>
<td><strong>Transfer to queue flow</strong></td>
<td>Use to manage what the agent experiences when transferring to another queue. This type of flow is associated with transfer to queue quick connects, and often plays messaging, then completes the transfer using the <strong>Transfer to queue</strong> block. This flow works with voice, chat, and tasks.</td>
</tr>
</tbody>
</table>

**Important**

- Do not place any sensitive information in this flow. When a cold transfer occurs, the transferring agent disconnects before transfer is completed, and this flow is run on the caller. This means information in the flow is played to the caller, not the agent.

### Create an inbound flow

Use these steps to create an inbound flow.

1. In the left navigation menu, choose **Routing, Flows**.
2. Choose **Create flow**. This opens the flow designer and creates an inbound flow (Type = Flow).

3. Type a name and a description for your flow.

4. Search for a flow block using the **Search** bar, or expand the relevant group to locate the block. For descriptions of the contact blocks, see [Flow block definitions](#).

5. Drag and drop contact blocks onto the canvas. You can add blocks in any order or sequence, as connections between elements aren't required to be strictly linear.

![Amazon Connect Flow Designer](image)

**Tip**

You can move blocks around the canvas so the layout aligns to your preferences. To select multiple blocks at the same time, press the **Ctrl** key on your laptop (or the **Cmd** key on a Mac), choose the blocks you want, and then use your mouse to drag them as a group within the flow. You can also use the **Ctrl/Cmd** key to start at one point on the canvas and drag your pointer across the canvas to select all blocks included in the frame.

6. Double-click the title of the block. In the configuration pane, configure settings for that block and then choose **Save** to close the pane.

7. Back on the canvas, click on the first (the originating) block.

8. Choose the circle for the action to perform, such as Success.

9. Drag the arrow to the connector of the group that performs the next action. For groups that support multiple branches, drag the connector to the appropriate action.

10. Repeat the steps to create a flow that meets your requirements.
11. Choose **Save** to save a draft of the flow. Choose **Publish** to activate the flow immediately.

**Note**

All connectors must be connected to a block in order to successfully publish your flow.

**Use the mini-map to navigate a flow**

In the lower left corner of the flow designer, there's a miniaturize view of the entire flow. Use this view to help you easily navigate the flow. The drag-to-move mini-map has visual highlights that enable you to quickly move to any point in the flow.

The following image shows the location of the mini-map in the flow designer. The arrow points to the toggle that you use to hide or show the mini-map.

![Mini-map Image](image-url)

The following GIF shows an example of how you can use the mini-map to navigate a large flow. Click or tap the mini-map to move the view to the desired location on the flow designer.
Note the following functionality:

- It shows your current view in green outline.
- It highlights selected blocks in blue, notes in yellow, search results in orange, and termination blocks in black.
- It allows continuous movement of the view when you drag on the mini-map.
- It returns the view to the Entry block and trims unused space when you choose Reset.

**Customize the name of a block**

To help you distinguish blocks in a flow, you can customize the names of blocks. For example, when there are multiple Play prompt blocks, and you want to distinguish between them at a glance you can assign each block their own name.

Custom flow block names appear in CloudWatch logs under the Identifier field. This makes it easier for you to review the logs to diagnose issues.

⚠️ **Important**

- The following characters are not allowed in the block name or Identifier field: (%: \(/) = $; []; {}
The following strings are not allowed in the block name or Identifier field: __proto__, constructor, __defineGetter__, __defineSetter__, toString, hasOwnProperty, isPrototypeOf, propertyIsEnumerable, toLocaleString, and valueOf.

There are two ways you can specify a custom block name:

- On the block, choose ..., and then choose **Add block name**, as shown in the following GIF.

- You can also customize the name of the block on the **Property** page, as shown in the following GIF.
Undo and redo actions in the flow designer

You can undo and redo actions in the flow designer. Choose the undo and redo items on the toolbar. Or, with your cursor on the flow designer canvas, use the shortcut keys: Ctrl+Z to undo, Ctrl+Y to redo.

Tip

On a Mac, Ctrl+Y opens the history page instead of performing a redo.

To access a history of your actions that you can undo, choose the **Undo** dropdown button on the toolbar, as shown in the following image.
Limits

<table>
<thead>
<tr>
<th>Action</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>History limit</td>
<td>Up to 100 actions can be undone.</td>
</tr>
<tr>
<td>Dragging unconnected connector</td>
<td>This action cannot be undone.</td>
</tr>
<tr>
<td>Folding of notes</td>
<td>This action cannot be undone.</td>
</tr>
<tr>
<td>Page reload</td>
<td>The undo history is not retained after a page is reloaded.</td>
</tr>
</tbody>
</table>

Add notes to a block

To add notes to a block, on the toolbar choose **Annotation**. Or, with your cursor on the flow designer canvas, use the shortcut keys: Ctrl + Alt +N. A yellow box opens for you to type up to 1000 characters. This enables you to leave comments that others can view.

The following image shows the flow designer toolbar, the annotation box, and an annotation that is attached to a block.
The following GIF shows how to move notes around the flow designer and attach them to a block.

The following image shows the dropdown menu that allows you to view a list of all the notes in a flow. Choose a note to navigate to it. Use the search box to search notes across the flow.
Note the following functionality:

- Unicode and emojis are supported.
- You can copy and paste, undo, and redo into the note box.
- You can search notes across the flow.
- When a block is deleted, the notes are deleted. When a block is restored, the notes are restored.

### Limits

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character limit</td>
<td>1000 characters per note</td>
</tr>
<tr>
<td>Attachment limit</td>
<td>5 notes per block</td>
</tr>
<tr>
<td>Note limit</td>
<td>100 notes per flow</td>
</tr>
</tbody>
</table>

### Copy and paste flows

You can select, cut, copy, and paste a complete flow or multiple blocks within or across flows. The following information is copied:

- All configured settings in the selected flow blocks.
- The layout arrangements.
The following image shows the copy item on the flow designer toolbar.

Or, if desired, use the shortcut keys.

**Windows: CTRL+C to copy, CTRL+V to paste, and CTRL+X to cut**

1. To select multiple blocks at the same time, press the Ctrl key, and choose the blocks you want.
2. With your cursor on the flow designer canvas, press Ctrl+C to copy the blocks.
3. Press CTRL+V to paste the blocks.

**Mac: Cmd+C to copy, Cmd+V to paste, and Cmd+X to cut**

1. To select multiple blocks at the same time, press the Cmd key, and choose the blocks you want.
2. Press Cmd+C to copy the blocks.
3. Press Cmd+V to paste the blocks.

⚠️ **Tip**

Amazon Connect uses the clipboard for this feature. Paste won't work if you edit the JSON in your clipboard and introduce a typo or other error, or if you have multiple items saved to your clipboard.
Archive, delete, and restore flows

Flows and modules must be archived before you can delete them from your Amazon Connect instance. Archived flows and modules can be restored.

⚠️ Warning
Deleted flows and modules cannot be restored. They are permanently deleted from your Amazon Connect instance.

Important things to know

- **Use caution when archiving flows or modules.** Amazon Connect does not validate whether the flow or module you are archiving is being used in other published flows. It does not warn you that the flow is in use.

- Default flows cannot be archived or deleted. If you attempt to archive a default flow, you'll get message similar to the following image.

  ![Default flow cannot be archived](image)

- Flows and modules that are associated with queues, quick connects, or phone numbers cannot be archived. You need to disassociate the resources from the flows before you can archive them.

- Archived flows and modules count towards your Flows per instance and Modules per instance service quotas. You must delete them to not have them counted. For more information about quotas, see Amazon Connect service quotas.

Archive a flow or module

There are two ways you can archive flows or modules.
Option 1: Open the flow or module and then archive it

1. Log in to Amazon Connect with a user account that has the **Numbers and flows - Flows - Edit** permission in its security profile. If you are archiving a flow module, you need **Flow modules - Edit** permission.

2. On the navigation menu, choose **Routing, Flows**.

3. Open the flow or module you want to archive.

4. On the flow designer page, choose the dropdown menu, and then choose **Archive**, as shown in the following image.

![Flow designer page with Archive option highlighted](image)

5. Confirm you want to archive the flow or module.

6. To locate the archived flow or module, choose **View archive**.

Option 2: Search for flow or module and then archive it

- On the **Flows** page, search for the flow or module you want archive, and then choose **Archive** from the ... menu, as shown in the following image.

![Flows page with Archive option highlighted](image)
Restore an archived flow or module

There are two ways you can restore flows or modules.

Option 1: View list of archived flows or modules, and choose Restore

1. Log in to the Amazon Connect admin website with a user account that has the **Numbers and flows - Flows - Edit** permission in its security profile. If you are restoring a flow module, you need **Flow modules - Edit** permission.

2. On the navigation menu, choose **Routing, Flows**.

3. On the **Flows** page, choose **View archive**.

   - To restore archived modules, on the **Flows** page, choose the **Modules** tab, and then choose **View archive**.

4. On the **Flows Archive** page, next to the flow or module you want to restore, under **Actions**, choose ... and then choose **Restore**. This option is shown in the following image.

![Flows Archive](image)

Option 2: Restore the archived flow or module from the flow designer

1. Open the archived flow or module in the flow designer.

2. From the dropdown menu, choose **Restore**, as shown in the following image.

![Archived - Sample](image)
Delete an archived flow or module

You can delete archived flows and modules manually by using the Amazon Connect admin website, or programmatically by using the `DeleteContactFlow` API.

⚠ **Warning**

Deleted flows and modules cannot be restored. They are permanently deleted from your Amazon Connect instance.

**Option 1: View list of archived flows or modules, and choose Delete**

1. Log in to the Amazon Connect admin website with a user account that has the **Numbers and flows - Flows - Remove** permission in its security profile. If you are deleting a flow module, you need **Flow modules - Remove** permission.
2. On the navigation menu, choose **Routing, Flows**.
3. On the **Flows** page, choose **View archive**.
   - To delete modules, on the **Flows** page, choose the **Modules** tab, and then choose **View archive**.
4. On the **Flows Archive** page, next to the flow or module you want to delete, under **Actions**, choose ... and then choose **Delete**.
5. Confirm that you want to delete the flow or module.

**Option 2: Delete the archived flow or module from the flow designer**

1. Open the archived flow or module in the flow designer.
2. From the dropdown menu, choose **Delete**.
3. Confirm that you want to delete the flow or module.

**Generate logs**

After your flow is published live, you can use flow logs to help analyze flows and quickly find errors your customers encounter. If needed, you can roll back to a previous version of the flow.

For more information about using flow logs, see [Track events as customers interact with flows](#).
Flow version control: Roll back a flow

View a previous version of a flow

This procedure is especially useful if you want to research how a flow has been changed over time.

1. In the flow designer, open the flow you want to view.
2. Choose the **Latest: Published** dropdown to view a list of previously published versions of the flow.
   
   For default flows that are provided with your Amazon Connect instance, the oldest flow in the list is the original version. The date matches when your Amazon Connect instance was created. For example, in the following image, the original default flow is dated 07/21/22.

![Default agent hold](image)

3. Choose the version of the flow to open and view it. You can view all the blocks and how they are configured.
4. Next, you can do one of the following:

   - To return to the most recently published version, choose it from the **Latest: Published** dropdown list.
   
   - Make changes to the previous version and choose **Save as** from the dropdown to save it with a new name. Or choose **Save** from the dropdown to assign the same name.
Or, choose **Publish** to return the previous version to production.

**Roll back a flow**

1. In the flow designer, open the flow you want to roll back.
2. Use the drop-down to choose the version of the flow you want to roll back to. If you choose **Latest**, it reverts the flow to the most recent published version. If there isn't a published version, it reverts to the most recent saved version.

   ![](image)

   **Note**
   
   To see a consolidated view of all changes across all flows, click the **View historical changes** link at the bottom of the Flows page. You can filter to a specific flow by date or user name.

3. Choose **Publish** to push that version into production.

**Contact initiation methods and flow types**

Every contact in your Amazon Connect contact center is initiated by one of the following methods:

- Inbound
- Outbound
- Transfer
- Callback
- API
• Queue_Transfer
• Disconnect

You can create flows appropriate for a given initiation method when you know which types of flows the initiation method uses.

For each initiation method, this topic explains which types of flows are run.

**Inbound**

The customer initiated a voice (phone) contact with your contact center.

• When the contact successfully connects with the phone number of your contact center, an **Inbound flow** is presented to caller.
• During the transition in the **Inbound flow**, if the customer is put in a queue, a **Customer queue flow** is played to customer.
• After the agent becomes available to handle the caller and accept the contact, a **Agent whisper flow** is played to the agent.
• After a **Agent whisper flow** completes, a **Customer whisper flow** is played to customer.
• After the both whisper flows are played successfully to the agent and the customer respectively, the caller gets connected to agent for interaction.

To summarize, for a simple inbound call, the following flow types are played before caller is connected to agent:

1. **Inbound flow**
2. **Customer queue flow**
3. **Agent whisper flow**
4. **Customer whisper flow**

**Outbound**

An agent initiated voice (phone) contact to an external number, by using their CCP to make the call.

• As soon as the destination party picks the call, they are presented with an **Outbound whisper flow**.
• After an **Outbound whisper flow** successfully completes, the agent and the contact are connected for interaction.

To summarize, an **Outbound flow** type is the only one involved in an outbound call initiated from Amazon Connect.

**Transfer**

The contact was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.

Before the agent transfers the contact to another agent or queue, all the flows involved in an INBOUND contact are run.

• Agent to Agent transfer using Agent Quick Connect
  
• After the agent transfers the inbound contact to another agent:
  
  • A **Agent transfer flow** is played to the source agent.
  
  • After the destination agent accepts the call, a **Agent whisper flow** is played to destination agent, and then a **Customer whisper flow** is played to source agent.
  
  • After all three flows are successfully run, the interaction begins between the source and destination agents.
  
  • During this whole process, the inbound caller is on hold and a **Customer hold flow** is played to the inbound caller during hold time.

After the source agent is connected with destination agent, the source agent can do one of the following actions:

• Choose **Join**. This joins all parties on the call: source agent, destination agent, and the customer are joined in a conference call.

• Choose **Hold all**. This puts the destination agent and the customer on hold.

• Put destination agent on hold, so only the source agent can talk to the customer.

• Choose **End call**. The source agent leaves the call but the destination agent and the customer are directly connected and continue talking.

To summarize for an agent to agent transfer call, the following flow types are run:

1. **Agent transfer flow**

2. **Agent whisper flow** (played to the destination agent)
3. **Customer whisper flow** (played to the source agent) during whole this process

4. **Customer hold flow** played to the original caller

- Agent to Queue transfer using Queue Quick Connect
  - After the agent transfers the inbound call to another queue:
    - A **Queue transfer flow** is played to source agent.
    - After the agent from the transferred queue accepts the call, an **Agent whisper flow** is played to destination agent, and then a **Customer whisper flow** is played to source agent.
    - After these flows run, the source and destination agent interaction begins.
    - During this whole process, the inbound caller is on hold. A **Customer hold flow** is played to the inbound caller during the hold time.

After the source agent is connected with destination agent, the source agent can do one of the following:

- Choose **Join**. This joins all parties on the call: source agent, destination agent, and the customer are joined in a conference call.
- Choose **Hold all**. This puts destination agent and the customer on hold.
- Put destination agent on hold, so only the source agent can talk to the customer.
- Choose **End call**. The source agent leaves the call but the destination agent and the customer are directly connected and continue talking.

To summarize for agent to queue transfer call, the following flows are played:

1. **Queue transfer flow**
2. **Agent whisper flow** (played to the destination agent)
3. **Customer whisper flow** (played to the source agent) during whole this process
4. **Customer hold flow** played to the original caller

**Callback**

The customer is contacted as part of a callback flow.

- As soon as agent accepts the callback contact, an **Agent whisper flow** is played to the agent.
- After the customer accepts the callback call, an **Outbound whisper flow** is played to customer.

- After these two flows are played, the agent and customer are connected and can interact.
To summarize, for callback contacts, the following flow types are played:

- **Agent whisper flow**
- **Outbound whisper flow**

## API

The contact was initiated with Amazon Connect by API. This could be:

1. An outbound contact you created and queued to an agent using the `StartOutboundVoiceContact` API.
2. A live chat that was initiated by the customer with your contact center where you called the `StartChatConnect` API.
3. A task that was initiated by calling the `StartTaskConnect` API.

Following is an example of an API initiated contact method:

- After the outbound contact is successfully initiated using the `StartOutboundVoiceContact` API, an **Inbound flow** provided in the API request is played to the customer.

- Depending on the configuration of the **Inbound flow**, additional flows are played. For example, an **Inbound flow** transfers a customer to an agent for conversation. In this case, a **Customer queue flow** is played to customer while they waiting in queue for an agent.

- When the available agent accepts the call, an **Agent whisper flow** is played to agent.

- A **Customer whisper flow** is played to customer.

- After both whisper flows are played successfully to the agent and customer respectively, the caller is connected to agent for interaction.

To summarize API initiation methods, the following flows are played before the customer is connected to agent:

- **Inbound flow**
- **Customer queue flow**
- **Agent whisper flow**
- **Customer whisper flow**
Queue_Transfer

While the customer was in one queue (listening to a Customer queue flow), they were transferred into another queue using a flow block.

- The customer who is waiting in the queue for an agent is presented only with a Customer queue flow. No additional flows are involved.

Disconnect

When a Set disconnect flow block runs, it specifies which flow to run after a disconnect event during a contact.

- You can specify only an Inbound contact flow in this block. Since it occurs after the disconnect event, no additional flow is presented to customer.

Override the default contact flows

For all of the initiation methods discussed in this topic, if you don't specify flows for Agent whisper flow, Customer whisper flow, Customer queue flow, or Outbound whisper flow, then the default flow of that type runs instead. For a list of default flows, see Default flows.

To override the defaults and use your own flows, use the following blocks:

- Set customer queue flow
- Set hold flow
- Set whisper flow

For more information, see Default flows.

Attach a claimed or ported phone number to a flow

After you publish a flow, you can attach a claimed or ported phone number to it. When a contact calls the phone number that you associate with a flow, they are connected to that flow.
To associate a claimed or ported phone number with a published flow

1. Log in to your Amazon Connect instance (https://instance name.my.connect.aws/) with an Admin account or a user account that has Phone number - Edit permissions in it's security profile. (To find the name of your instance, see Find your Amazon Connect instance ID/ARN.)

2. On the navigation menu, choose Channels, Phone numbers.

3. Locate the phone number to associate with the flow in the list. Click the phone number to open the Edit Phone number page. The following image shows a sample phone number that you would click.

4. On the Edit Phone number page, do the following:
   a. (Optional) Edit the description for the phone number.
   b. For Flow / IVR, select the flow. Note that only published flows are included in this list.
   c. Choose Save.

Flow modules for reusable functions

Flow modules are reusable sections of a flow. You can create them to extract repeatable logic across your flows, and create common functions. For example:

1. You can create a module that sends SMS text messages to customers.
2. You can invoke the module in flows that handle situations where customers want to reset their passwords, check their bank balances, or receive a one-time password.

Following are the benefits of using modules:

- Simplify managing common functionality across flows. For example, an SMS module could validate the format of phone number, confirm SMS opt-in preferences, and integrate with an SMS service, such as Amazon Pinpoint.
• Makes it more efficient to maintain flows. For example, you can quickly propagate changes across all flows that invoke a flow module.

• Helps separate flow designer responsibilities. For example, you can have both technical module designers and non-technical flow designers.

**Where you can use modules**

You can use modules in any flow that is type **Inbound flow**.

The following types of flows do not support modules: **Customer queue, Customer hold, Customer whisper, Outbound whisper, Agent hold, Agent whisper, Transfer to agent, Transfer to queue**.

**Limitations**

• Modules do not allow overriding flow local data of the invoking flow. This means you can’t use the following with modules:
  • External attributes
  • Amazon Lex attributes
  • Customer Profiles attributes
  • Amazon Q in Connect attributes
  • Queue metrics
  • Stored customer input
• Modules do not allow invoking another module.

To pass any data to a module, or to get any data from a module, you need to pass and retrieve attributes.

For example, you want data that is written from Lambda (an External attribute) and pass it to the module so you can make a decision. Your Lambda identifies whether the customer is a VIP member. You need that information inside the module because if they are a VIP member, you want to play a prompt thanking them for their membership. Since default Lambda is not available inside a module, you use attributes to pass and retrieve data.
Security profile permissions for modules

Before you can add modules to Inbound flows, you must have permissions in your security profile. By default, the Admin and CallCenterManager security profiles have these permissions.

Create a module

For information about the number of modules that you can create for each Amazon Connect instance, see Amazon Connect service quotas.

1. Log in to the Amazon Connect console with an account assigned to a security profile that has permissions to create modules.
2. On the navigation menu, choose Routing, Contact flows.
3. Choose Modules, Create flow module.
4. Add the blocks that you want to your module. When finished, choose Publish. This makes the module available to use in other flows.

Add a module to a flow

1. Log in to the Amazon Connect console with an account assigned to a security profile that has permissions to create flows. You don't need permissions to create modules.
2. On the navigation menu, choose Routing, Contact flows.
3. Choose Create flow or select an existing flow that is an Inbound type.
4. To add a module, go to the Integrate section, and choose Invoke flow module.
5. When you're finished creating your flow, choose Publish.

Example module

This module shows how to get a random fun fact by invoking a Lambda function. The module uses a contact attribute ($.Attributes.FunFact) to retrieve the fun fact. Flows that invoke this module can play a FunFact to customers, depending on their incoming contact type.

The inbound flows in your instance can invoke this common module and get the fun fact.

Following is an image of the FunFact module:
Create prompts

Prompts are audio files played in call flows. For example, hold music is a prompt. Amazon Connect comes with a set of prompts that you can add to your flows. Or, you can add your own recordings.

We recommend that you align your prompts and routing policies with each other to ensure a smooth call flow for customers.

You can create and manage prompts by using the Amazon Connect admin site as described in the topics in this section. Or you can use the Prompt actions documented in the Amazon Connect API Reference Guide.

Contents

- How to create prompts
- Supported file types
How to create prompts

This topic explains how to use the Amazon Connect admin website to create prompts. To create prompts programmatically, see `CreatePrompt` in the *Amazon Connect API Reference Guide*.

1. Log in to Amazon Connect using an account that has the following security profile permission:
   - **Numbers and flows, Prompts - Create**
2. On the navigation menu, choose **Routing, Prompts**.
3. On the **Prompts** page, choose **Add prompt**.
4. On the **Add Prompt** page, enter a name for the prompt.
5. In the **Description** box, describe the message. We recommend using this box to provide a detailed description of the prompt. It is helpful for accessibility.
6. Choose the following actions:
   - **Upload**—Select **Choose File** to upload a .wav file that you have legal permission to use.
   - **Record**—Choose **Start recording** and speak into your microphone to record a message. Choose **Stop recording** when you're finished. You can choose **Crop** to cut sections of the recorded prompt or choose **Clear recording** to record a new prompt.
7. In the **Prompt Settings** section, enter any tags you want to use to manage the prompt.

For example, you may have a department that manages prompts for greetings. You can tag those prompts so users can focus on only those recordings that pertain to them.
Use the filters on the **Prompts** page to filter the list of prompts by **Name**, **Description**, and **Tags**. To copy the full Amazon Resource Name (ARN) of a prompt with just one click, choose the **Copy** icon. When you set up dynamic prompts in a flow, you'll need to enter the full ARN of the prompt.

**Supported file types**

You can upload a pre-recorded .wav file to use for your prompt, or record one in the web application.

We recommend using 8 KHz .wav files that are less than 50 MB and less than 5 minutes long. If you use higher rated audio libraries, such as 16 KHz or 16 bit files, Amazon Connect has to down sample them into 8 KHz samples because of PSTN limitations. This may result in low quality audio. For more information, see the following Wikipedia article: [G.711](https://en.wikipedia.org/wiki/G.711).

**Maximum length for prompts**

Amazon Connect supports prompts that are less than 50 MB and less than 5 minutes long.

**Bulk upload of prompts not supported in UI, API, or CLI**

Currently, bulk uploading of prompts is not supported through the Amazon Connect console or programmatically using the API or CLI.

**Add text-to-speech to prompts**

You can enter text-to-speech prompts in the following flow blocks:
Amazon Polly converts text-to-speech

To convert text-to-speech, Amazon Connect uses Amazon Polly, a service that converts text into lifelike speech using SSML.

Amazon Polly default voices such as Amazon Polly Neural and Standard voices are **free**. You are charged only for using custom voices such as unique **Brand Voices** that are associated with your account.

Amazon Polly best sounding voice

Amazon Polly periodically releases improved voices and speaking styles. You can choose to automatically resolve your text-to-speech to the most lifelike and natural sounding variant of a voice. For example, if your flows use Joanna, Amazon Connect automatically resolves to Joanna's conversational speaking style.

**Note**

If no Neural version is available, Amazon Connect defaults to the standard voice.

To automatically use the best sounding voice

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).
2. If prompted to login, enter your AWS account credentials.
3. Choose the name of the instance from the **Instance alias** column.
4. In the navigation pane, choose Flows.

5. In the Amazon Polly section, choose Use the best available voice.

**How to add text-to-speech**

1. In a flow, add the block that will play the prompt. For example, add a Play prompt block.
2. In the Properties, choose Text-to-speech.
3. Enter plain text. For example, the following image shows Thank you for calling.

Or enter SSML, as shown in the following image:
SSML-enhanced input text gives you more control over how Amazon Connect generates speech from the text you provide. You can customize and control aspects of speech such as pronunciation, volume, and speed.

For a list of SSML tags you can use with Amazon Connect, see SSML tags supported by Amazon Connect.

For more information about Amazon Polly, see Using SSML in the Amazon Polly Developer Guide.

**Create dynamic text strings in Play prompt block**

Use a Play prompt block to use an audio file to play as a greeting or message to callers. You can also use contact attributes to specify the greeting or message delivered to callers. To use the values of a contact attribute to personalize a message for a customer, include references to stored or external contact attributes in the text-to-speech message.

For example, if you retrieved the customer's name from a Lambda function, and it returns values from your customer database for FirstName and LastName, you could use these attributes to say the customer's name in the text-to-speech block by including text similar to the following:

- Hello $.External.FirstName $.External.LastName, thank you for calling.

This message is shown in the following image of the text-to-speech box of the Play prompt block.
Alternatively, you could store the attributes returned from the Lambda function using a **Set contact attributes** block, and then reference the user-defined attribute created in the text-to-speech string.

If you are referencing a user-defined attribute that was previously set as a contact attribute in the flow using the API, you can reference the attribute using the `$Attributes.nameOfAttribute` syntax.

For example, if the contact in question has attributes "FirstName" and "LastName" set previously, reference them as follows:

- **Hello $.Attributes.FirstName $.Attributes.LastName, thank you for calling.**

### Dynamically select which prompts to play

You can dynamically select which prompt to play by using an attribute.

1. Add **Set contact attributes** blocks to your flow. Configure each one to play the appropriate audio prompt. For example, the first one might play the .wav file when your contact center is open. The second one might play the .wav file for when it's closed.

The following image shows how you might configure a **Set contact attributes** block. In this example, the user-defined attribute is named **CompanyWelcomeMessage**. You can name your attribute anything you want.
2. In the **Play prompt** block, choose **User Defined**, and then enter the name of the attribute that you created in step 1, as shown in the following image.
3. Connect the **Set contact attributes** blocks to the **Play prompt** block. The following example shows how it might look if you added one of each block to test how this works.

### Set up prompts to play from an S3 bucket

When you configure prompts on the **Get customer input**, **Loop prompts**, **Play prompt**, or **Store customer input** blocks, you can choose an S3 bucket as the source location. You can store as many
voice prompts as needed in an S3 bucket and access them in real time by using contact attributes. For examples, see the Play prompt block.

Requirements

- **Supported formats**: Amazon Connect supports .wav files to use for your prompt. You must use .wav files that are 8KHz, and mono channel audio with U-Law encoding. Otherwise, the prompt won't play correctly. You can use publicly available third-party tools to convert your .wav files to U-Law encoding. After converting the files, upload them to Amazon Connect.

- **Size**: Amazon Connect supports prompts that are less than 50MB and less than five minutes long.

- **For Regions that are disabled by default** (also called opt-in Regions) such as Africa (Cape Town), your bucket must be in the same Region.

Update the S3 bucket policy

To allow Amazon Connect to play prompts from an S3 bucket, when you set up your S3 bucket, you must update the bucket policy to grant connect.amazonaws.com (the Amazon Connect service principal) permission to call s3:ListBucket and s3:GetObject.

**To update the S3 bucket policy:**

1. Go to the Amazon S3 admin console.
2. Choose the bucket that has your prompts.
3. Choose the **Permissions** tab.
4. In the **Bucket policy** box, choose **Edit**, and paste the following policy as your template. Replace the bucket name, Region, AWS account ID, and **instance ID** with your own information, and then choose **Save changes**.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "Service": "connect.amazonaws.com"
            }
        }
    ]
}
```
5. Encryption: Amazon Connect cannot download and play prompts from an S3 bucket if an AWS managed key is enabled on that S3 bucket. However, you can use a customer managed key to allow the Amazon Connect service principal ("connect.amazonaws.com") that enables your Amazon Connect instance to access the S3 bucket. See the following code snippet:

```json
{
    "Sid": "Enable Amazon Connect",
    "Effect": "Allow",
    "Principal": {
        "Service": "connect.amazonaws.com"
    },
    "Action": "kms:decrypt",
    "Resource": [
        "arn:aws:kms:region:account-ID:key/key-ID"
    ]
}
```

For information on how to find the key ID, see [Finding the key ID and key ARN](https://docs.aws.amazon.com/kms/latest/developerguide/finding-key-ids.html) in the *AWS Key Management Service Developer Guide*.

After you set up your S3 bucket with the required bucket policy, configure [Get customer input](https://aws.amazon.com/connect/guide/#get-customer-input), [Loop prompts](https://aws.amazon.com/connect/guide/#loop-prompts), [Play prompt](https://aws.amazon.com/connect/guide/#play-prompt), or [Store customer input](https://aws.amazon.com/connect/guide/#store-customer-input) to play a prompt from the bucket.
Choose the voice for audio prompts

You select the text-to-speech voice and language in the Set voice block.

You can also use SSML in Amazon Lex bots to modify the voice used by a chat bot when interacting with your customers. For more information about using SSML in Amazon Lex bots, see Managing Messages and Managing Conversation Context in the Amazon Lex Developer Guide.

Tip

If you enter text that isn't supported for the Amazon Polly voice you are using, it won't be played. However, any other supported text in the prompt will be played. For a list of supported languages, see Languages Supported by Amazon Polly.

Use SSML tags to personalize text-to-speech

When you add a prompt to a flow, you can use SSML tags to provide a more personalized experience for your customers. SSML tags are a way to control how Amazon Polly generates speech from the text you provide.

The default setting in a flow block for interpreting text-to-speech is Text. To use SSML for text to speech in your flow blocks, set the Interpret as field to SSML as shown in the following image.
SSML tags aren't interpreted in chats

If you create text-to-speech text and apply SSML tags, they won't be interpreted in a chat conversation. For example, in the following image both the text and tags will be printed in the chat conversation.
## SSML tags supported by Amazon Connect

Amazon Connect supports the following SSML tags.

### Tip

If you use an unsupported tag in your input text, it's automatically ignored when it's processed.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Use to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>speak</td>
<td>All SSML-enhanced text must be enclosed within a pair of speak tags.</td>
</tr>
<tr>
<td>break</td>
<td>Add a pause to your text. The maximum duration for a pause is 10 seconds.</td>
</tr>
<tr>
<td>lang</td>
<td>Specify another language for specific words.</td>
</tr>
<tr>
<td>mark</td>
<td>Put a custom tag within the text.</td>
</tr>
<tr>
<td>p</td>
<td>Add a pause between paragraphs in your text.</td>
</tr>
<tr>
<td>phoneme</td>
<td>Make a phonetic pronunciation for specific text.</td>
</tr>
<tr>
<td>prosody</td>
<td>Control the volume, rate, or pitch of your selected voice.</td>
</tr>
<tr>
<td>s</td>
<td>Add a pause between lines or sentences in your text.</td>
</tr>
<tr>
<td>say-as</td>
<td>Combine with the interpret-as attribute to tell Amazon Polly how to say certain characters, words, and numbers.</td>
</tr>
<tr>
<td>sub</td>
<td>Combine with the alias attribute to substitute a different word (or pronunciation) for</td>
</tr>
</tbody>
</table>
### Tag and Pronunciation

<table>
<thead>
<tr>
<th>Tag</th>
<th>Use to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>selected text such as an acronym or abbreviation.</td>
</tr>
<tr>
<td>w</td>
<td>Customize the pronunciation of words by specifying the word's part of speech or alternate meaning.</td>
</tr>
<tr>
<td>amazon:effect name=&quot;whispered&quot;</td>
<td>Indicate that the input text should be spoken in a whispered voice rather than as normal speech.</td>
</tr>
</tbody>
</table>

If you use an unsupported tag in your input text it is automatically ignored when it is processed.

To learn more about the SSML tags, see [Supported SSML Tags](#) in the Amazon Polly Developer Guide.

### Neural and Conversational Speaking Styles

For the **Joanna** and **Matthew** neural voices, in American English (en-US), you can also specify a [Conversational speaking style](#) or a [Newscaster speaking style](#).

### Set up contact transfers

Amazon Connect enables you to set up different kinds of transfers:

- **Agent-to-agent transfers**: For example, if you want agents to be able to transfer calls or tasks to other agents.
- **Transfers to a specific agent**: For example, if you want to route contacts to the last agent the customer interacted with, or route contacts to agents who have specific responsibilities.
- **Transfers to queues**: For example, if you want to transfer the contact to a sales, support, or escalation queue. To do this, create a [queue quick connect](#). This works with voice, chat, and task contacts.
- **Transfers to phone numbers**: For example, if you want to transfer the contact to a phone number, such as an on-call pager. To do this, create an phone number quick connect.
Overview of steps

To set up call transfers and quick connects

1. Choose a flow type based on what you want to do: Transfer to agent or Transfer to queue. Phone number transfers do not require a specific type of contact flow.

2. Create and publish the flow.

3. Create a quick connect for the type of transfer to enable: Agent, Queue, or Phone number.

   When you create the Agent or Queue quick connect, select a flow that matches the type of transfer to enable. Phone number quick connects require only a phone number, and do not allow you to set a queue or flow.

4. Add the quick connect that you created to any queue used in a flow for which to enable contact transfer, such as the queue used in the flow for incoming contacts.

5. Make sure the queue is in a routing profile assigned to the agents who transfers contacts.

Create quick connects

Quick connects are a way for you to create a list of destinations for common transfers. For example, you might create a quick connect for Tier 2 support. If agents in Tier 1 support can't solve the issue, they will transfer the contact to Tier 2.

How many quick connects can I create? To view your quota of Quick connects per instance, open the Service Quotas console at https://console.aws.amazon.com/servicequotas/.

Types of quick connects

The type of a quick connect specifies the destination. You can specify one of the following destinations.

Phone number quick connect

Contacts are transferred to a phone number (such as an on-call pager).

User quick connect

Contacts are transferred to a specific user, such as an agent, as part of a flow.
**Important**

User and Queue quick connects only appear in the CCP when an agent goes to transfer a contact.

---

**Queue quick connect**

Contacts are transferred to a queue as part of a flow.

---

**Important**

User and Queue quick connects only appear in the CCP when an agent goes to transfer a contact.

---

**Step 1: Create quick connects**

Following are the instructions to add quick connects manually using the Amazon Connect console. To add quick connects programmatically, use the [CreateQuickConnect](https://aws.amazon.com/documentation/connect/) API.

**To add quick connects**

1. Log in to the Amazon Connect admin website at https://\*instance name\*.my.connect.aws/. To find the name of your instance, see [Find your Amazon Connect instance ID/ARN](https://aws.amazon.com/documentation/connect/).
2. On the navigation menu, choose **Routing, Quick connects**.
3. For each quick connect, do the following:
   a. Choose **Add new**.
   b. Enter a unique name. If desired, also enter a description.
   c. Choose a type.
   d. Enter the destination (for example, a phone number, the name of an agent, or the name of a queue).
   e. Enter a flow, if applicable.
   f. Enter a description.
4. When you're finished adding quick connects, choose **Save**.
Step 2: Enable agents to see quick connects

To enable your agents to see the quick connects in the CCP when they transfer a contact

1. After you create the quick connect, go to Routing, Queues and then choose the appropriate queue for the contact to be routed to.
2. On the Edit queue page, in the Quick connect box, search for the quick connect you created.
3. Select the quick connect and then choose Save.

Tip
Agents see the quick connects of the queues in their routing profile, including the Default outbound queue.

Example: Create a phone number quick connect to a mobile phone

In this example, you create a phone number quick connect to a person's mobile phone. This might be for a supervisor, for example, so agents can call them if needed.

Create a quick connect for a person's mobile phone number

1. On the navigation menu, choose Routing, Quick connects, Add quick connect.
2. On the Add quick connect page, enter a name for the quick connect, for example, John Doe's cell phone.
3. For Type, select Phone number.
4. For Phone number, enter the mobile phone number, starting with the country code. In the US, the country code is 1, as shown in the following image.
5. Choose **Save**.

Add the quick connect to a queue. Agents working this queue will see the quick connect in their CCP.

1. Go to **Routing, Queues**, and choose the queue you want to edit.
2. On the **Edit queue** page, in **Outbound caller ID number**, choose a number claimed for your contact center. This is required to make outbound calls.
3. At the bottom of the page, in the **Quick connect** box, search for the quick connect you created, for example, **John Doe's cell phone**.
4. Select the quick connect. In the following image of the **Edit queue** page, a phone number has been selected for the **Outbound caller ID number**, and **John Doe's cell phone** has been selected as the quick connect.
5. Choose Save.

Test the quick connect

1. Open the Contact Control Panel.
2. Choose Quick connects.
3. Select the quick connect you created, and then choose Call.
Delete quick connects

There are two ways you can delete a quick connect:

- Use Amazon Connect console. This topic provides instructions.
- Use the `DeleteQuickConnect` API.

To delete a quick connect

1. Log in to your Amazon Connect instance (https://instance name.my.connect.aws/) with an Admin account or a user account that has Quick connects - Delete permissions in its security profile. (To find the name of your instance, see Find your Amazon Connect instance ID/ARN.)
2. On the navigation menu, choose Routing, Quick connects.
3. Select the quick connect, and then choose the Delete icon.
If you don't see the delete option, check the following:

- You are using the latest Amazon Connect user interface. The following image shows a banner at the top of the **Quick connects** page. Choose **Try it now** to use the latest Amazon Connect user interface.

- You have **Quick connects - Delete** permission in your security profile.

### How quick connects work

This article explains how each type of quick connect works: agent, queue, and phone number quick connects. It explains which flows are used, and what appears on the agent's Contact Control Panel (CCP).

#### Tip

For all three types of quick connects, when the quick connect is invoked, the contact that the agent is working on hears the **Default customer hold** flow unless you specify a different customer hold flow.

### User quick connects

Let's say an agent named John is talking to a customer. During the conversation he needs to transfer the call to an agent named Maria. This is a user quick connect.

Here's what John and Maria do, and what flow blocks are triggered:

1. John chooses the **Quick Connect** button on his CCP. (On the earlier CCP, the button is named **Transfer**). He selects Maria from the list of quick connects.
When John does this, his CCP banner changes to **Connected**. However, the call isn't actually connected to Maria yet.

2. In our example scenario, Amazon Connect triggers an agent transfer flow that looks like the following image. It has the following blocks connected by **Success** branches: a **Play prompt**, a **Set whisper flow**, another **Set whisper flow**, and then a **Transfer to agent** block.

![Diagram of agent transfer flow](image)

The call is not yet connected to Maria.

3. John hears the first **Play prompt**, "Transferring to agent."

4. Maria receives a notification in her CCP to either accept or reject the call.

5. Maria accepts the incoming call. The banner in her CCP changes to **Connecting**.

6. The first **Set whisper flow** block is triggered. This block sets the custom agent whisper flow. It plays the Custom_Agent_Whisper to Maria, for example, "This is an internal call transferred from another agent."

   **Note**
   
   If you don't create and then select a custom agent whisper flow, Amazon Connect plays the **default agent whisper flow**, which says the queue name.

7. The next **Set whisper flow** block is triggered. It plays the Custom_Customer_Whisper to John, for example, "Your call is now connecting to an agent."

   **Note**
   
   If you don't create and then select a custom customer whisper flow, Amazon Connect plays the **default customer whisper flow**, which plays a beep.
8. Maria’s CCP banner shows she’s **Connected**. John and Maria are connected and can start talking.

9. Now John can do one of the following on his CCP:

   - Choose **Join**. This joins all parties on the call. John, Maria, and the customer have a conference call.
   - Choose **Hold all**. This puts Maria and the customer on hold.
   - Put Maria on hold, so he only talks to the customer.
   - Choose **End call**. He leaves the call but Maria and the customer are directly connected and continue talking.

**Queue quick connects**

Let’s say John is talking to a customer. The customer needs help resetting his password, so John needs to transfer him to the PasswordReset queue. This is a queue quick connect.

Another agent, Maria, is assigned to handle contacts in the PasswordReset queue. Her status in the CCP is **Available**.

Here’s what John and Maria do, and what flow blocks are triggered:

1. John chooses the **Quick Connect** button on his CCP. (On the earlier CCP, the button is named **Transfer**). He chooses to transfer the contact to the PasswordReset queue. As soon as John chooses the PasswordReset quick connect, his CCP banner shows **Connecting**.

⚠️ **Important**

Even though the status of the transferred call (internal-transfer) shows on John’s CCP banner as **Connecting**, the contact is not yet transferred to the PasswordReset queue.
2. Amazon Connect invokes the queue transfer flow that's associated with the PasswordReset quick connect. In this flow, the Transfer to queue block transfers the contact to the PasswordReset queue since it's specified in the block. The contact is now in the PasswordReset queue.

3. Maria is notified in her CCP to accept or reject the incoming call.

4. Maria accepts the incoming call and her CCP banner changes to Connecting.

5. The Agent whisper flow is played to Maria. It says "Connecting you to PasswordReset queue."

6. The Customer whisper flow is played to John. It says "Connecting you to PasswordReset queue."

7. Maria's CCP banner changes to Connected. John and Maria are connected and can start talking.

8. Now John can do one of the following from his CCP:
   - Choose Join. This joins all parties on the call. John, Maria, and the customer have a conference call.
   - Choose Hold all. This puts Maria and the customer on hold.
   - Put Maria on hold, so he only talks to the customer.
   - Choose End call. He leaves the call but Maria and the customer are directly connected and continue talking.

**Phone number quick connects**

There are no flows involved in a phone number quick connect. When an agent invokes an phone number quick connect, the call is directly connected the destination without invoking any flows.

Because no flow is involved in phone number quick connects, you can't set the outbound caller ID. Instead, the caller ID that you specified when you created the queue is used.

**Set up agent-to-agent transfers**

We recommend using these instructions to set up agent-to-agent voice, chat, and task transfers. You use a Set working queue block to transfer the contact to the agent's queue. The Set working queue block supports an omnichannel experience, whereas the Transfer to agent (beta) block does not.
Step 1: Create the quick connect

Following are the instructions to add quick connects manually using the Amazon Connect admin website. To add quick connects programmatically, use the CreateQuickConnect API.

Create a quick connect

1. On the navigation menu, choose Routing, Quick connects, Add a new destination.
2. Enter a name for the connect. Choose the type, and then specify the destination (such as a phone number or the name of an agent), flow (if applicable), and description.

   **Important**
   
   A description is required when you create a quick connect. If you don't add one, you'll get an error when you try to save the quick connect.

3. To add more quick connects, choose Add new.
4. Choose Save.
5. Go to the next procedure to enable your agents to see the quick connects in the Contact Control Panel (CCP).

Enable your agents to see the quick connects in the CCP when they transfer a contact

1. After you create the quick connect, go to Routing, Queues and then choose the appropriate queue for the contact to be routed to.
2. On the Edit queue page, in the Quick connect box, search for the quick connect you created.
3. Select the quick connect and then choose Save.

   **Tip**
   
   Agents see all of the quick connects for the queues in their routing profile.

Step 2: Set up the "Transfer to agent" flow

In this step, you create a flow that's type Transfer to agent and use a Set working queue block to transfer the contact to the agent.
1. On the navigation menu, choose **Routing, Flows**.

2. Use the drop-down to choose **Create transfer to agent flow**.

3. Type a name and a description for your flow.

4. In the left navigation menu, expand **Set**, and then drag the **Set working queue** block to the canvas.

5. Configure the **Set working queue** block as shown in the following image. Choose By agent, Set dynamically, Namespace = Agent, Value = User name.

   ![Set working queue block configuration](image.png)

   1. Choose **By agent**.
   2. Choose **Set dynamically**.
   3. For **Namespace**, use the dropdown box to select Agent.
   4. For **Value**, use the dropdown box to select User name.

6. Add a **Transfer to queue** block. You don't need to configure this block. The following image shows the **Success** branch of the **Set working queue** block connecting to the **Transfer to queue** block.
7. Save and publish this flow.

8. To show your agents how to transfer chats to another agent, see Transfer chats to another queue.

   To show your agents how to transfer tasks to another agent, see Transfer a task.

Resume a flow after transfer

Let's say you need to transfer a contact to an external department that's not using Amazon Connect. For example, maybe you need to transfer the caller to a shipping provider to check the status of their delivery. After the contact is disconnected from the phone number, you want them to be returned to your agent, for example, when the delivery company couldn't resolve their issue.

- For advanced creation, send tracking information as DTMF digits when the call is transferred, so that the shipment information is retrieved with the transferred call before the customer is connected.

To set up a flow for this scenario

1. Add a Transfer to phone number block to your contact flow.
2. In the Transfer to phone number block, enter the following settings:
   - Transfer to
     - Phone number—Sets the phone number to transfer the call to.
     - Set dynamically—Specify a contact attribute (choose a namespace and then a value) to set the phone number to transfer the call to.
   - Set timeout
• **Timeout (in seconds)**—The number of seconds to wait for the recipient to answer the transferred call.

• **Set dynamically**—Specify a contact attribute (choose a namespace and then a value) to use to set the *Timeout* duration.

• **Resume flow after disconnect**—When you select this option, after the call is transferred, the caller is returned to the flow when the call with the third party ends. Additional branches for *Success*, *Call failed*, and *Timeout* are added to the block when you select this option so that you can appropriately route contacts when there is an issue with the transfer.

**Optional parameters**

• **Send DTMF**—Select *Send DTMF* to include up to 50 Dual-Tone Multi-frequency (DTMF) characters with the transferred call. You can enter the characters to include, or use an attribute. Use the DTMF characters to navigate an automated IVR system that answers the call.

• **Caller ID number**—Specify the caller ID number used for transferred call. You can select a number from your instance, or use an attribute to set the number.

• **Caller ID name**—Specify the caller ID name used for the transferred call. You can enter a name, or use an attribute to set the name.

In some cases, the caller ID information is provided by the carrier of the party you are calling. The information may not be up-to-date with that carrier, or the number may get passed differently between systems because of hardware or configuration differences. If that is the case, the person you call may not see the phone number, or may see the name of a previously registered owner of the number, instead of the name you specify in the block.

3. Connect **Transfer to phone number** to the rest of your flow.

When the block executes:

1. The call is transferred to the phone number.

2. Optionally, when the conversation with the external party ends, the contact is returned to the flow.

3. The contact then follows the **Success** branch from the block to continue the flow.
4. If the call is not successfully transferred, one of the other branches is followed: **Call failed**, **Timeout**, or **Error**, depending on the reason the caller did not return to the flow.

**Manage contacts in a queue**

For inbound contacts, you can define advanced routing decisions to minimize queue wait times, or route contacts to specific queues, using blocks in your flow. For example:

- Use a **Check queue status** block to check staffing or agent availability for a queue before sending a contact to that queue.
- Or, use a **Get queue metrics** block to retrieve queue metrics.
- Then use a **Check contact attributes** block to check specific queue metric attributes, and define conditions to determine which queue to route the contact to based on attribute values. For more information about using queue metrics, see [Route based on number of contacts in a queue](#).

After determining which queue to transfer the contact to, use a **Transfer to queue** block in a flow to transfer the contact to that queue. When the **Transfer to queue** block runs, it checks the queue capacity to determine whether or not the queue is at capacity (full). This check for queue capacity compares the current number of contacts in the queue to the **Maximum contacts in queue** limit, if one is set for the queue. If no limit is set, the queue is limited to the number of concurrent contacts set in the **service quota** for the instance.

After the contact is placed in a queue, the contact remains there until an agent takes the contact, or until the contact is handled based on the routing decisions in your customer queue flow.

To change the queue associated with the call after it is already placed in a queue, use a **Loop prompts** block with a **Transfer to queue** block in a customer queue flow. In the block choose which queue to transfer the call to, or use an attribute to set the queue.

**To manage contacts in a queue using a Transfer to queue block**

1. In Amazon Connect, on the navigation menu choose **Routing, Flows**.
2. Choose the down arrow next to **Create flow**, then choose **Create customer queue flow**.
3. Under **Interact**, add a **Loop prompts** block to provide a message to the caller when the call is transferred, then every X seconds or minutes while the call is in the queue.
4. Select the **Loop prompts** block to display the settings for the block.
5. Choose **Add another prompt to the loop**.

6. Under **Prompts**, do one of the following:
   - Choose **Audio recording** in the drop-down menu, then select the audio recording to use as the prompt.
   - Choose **Text to Speech** in the drop-down menu, then enter text to use for the prompt in the **Enter text to be spoken** field.

7. To set an interrupt, choose **Interrupt every**, enter a value for the interrupt interval, and then choose a unit, either **Minutes** or **Seconds**. We recommend that you use an interval greater than 20 seconds to ensure that queued contacts that are being connected to an agent are not interrupted.

8. Choose **Save**.

9. Connect the block to the **Entry point** block in the contact flow.

10. Under **Terminate/Transfer**, drag a **Transfer to queue** block onto the designer.

11. Select the title of the block to display the settings for the block, then choose the **Transfer to queue** tab.

12. Under **Queue to check**, choose **Select a queue**, then select the queue to transfer calls to.

   Alternatively, choose **Set dynamically**, then reference an attribute to specify the queue. If you use an attribute to set the queue, the value must be the queue ARN.

13. Choose **Save**.

14. Connect the **Loop prompt** block to the **Transfer to queue** block.

15. Add additional blocks to complete the flow that you require, such as the blocks to check queue status or metrics, then choose **Save**.

   The flow is not active until you publish it.

---

⚠️ **Important**

To successfully complete the call transfer to another queue, you must include a block after the **Transfer to queue** block and connect the **Success** branch to it. For example, use an **End flow / Resume** block to end the flow. The flow does not end until the call is picked up by an agent.
Transfer contacts to a specific agent

Agent queues enable you to route contacts directly to a specific agent. Following are a couple of scenarios where you might want to do this:

- Route contacts to the last agent the customer interacted with. This provides a consistent customer experience.
- Route contacts to agents who have specific responsibilities. For example, you might route all billing questions to Jane.

**Note**

A queue is created for all users in your Amazon Connect instance, but only users who are assigned permissions to use the Contact Control Panel (CCP) can use it to receive contacts. The Agent and Admin security profiles are the only default security profiles that include permissions to use the CCP. If you route a contact to someone who doesn't have these permissions, the contact can never be handled.

**To route a contact directly to a specific agent**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. In the flow designer, open an existing flow, or create a new one.
3. Add a block in which you can select a queue to transfer a contact to, such as a **Set working queue** block.
4. Select the title of the block to open the block settings.
5. Select **By agent**.
6. Under **Select an agent**, enter the user name of the agent, or select the agent's user name from the drop-down list.
7. Choose **Save**.
8. Connect the **Success** branch to the next block in your flow.

You can also choose to use an attribute to select the queue created for the agent user account. To do so, after you choose **By agent**, choose **Use attribute**.
Use contact attributes to route contacts to a specific agent

When you use contact attributes in a flow to route calls to an agent, the attribute value must be either the agent's user name, or the agent's user ID.

To determine the user ID for an agent so that you can use the value as an attribute, use one of these options:

- Use the **Network** tab of the browser debugger to retrieve the agent ID. For example:
  1. In a Chrome browser, press F12 and go to the **Network** tab.
  2. In Amazon Connect, in the navigation menu, choose **Users, User management**, and then select an agent. Monitor the content of the **Network** tab. In the **Name** list, choose the GUID.
  3. Choose the **Preview** tab. The agent ID is displayed next to the **Id** field. The following image shows the location of the agent ID in the **Preview** tab.

- Use the **ListUsers** operation to retrieve the users from your instance. The agent's user ID is returned with the results from the operation as the value of the **Id** in the **UserSummary** object.

- Find the user ID for an agent by using **Amazon Connect agent event streams**. The agent events, which are included in the agent event data stream, include the agent ARN. The user ID is included in the agent ARN after **agent/**.

In the following agent event data, the agent ID is **87654321-4321-4321-4321-123456789012**.

```json
{
  "AWSAccountId": "123456789012",
```
"CurrentAgentSnapshot": {
  "AgentStatus": {
    "Name": "Available",
    "StartTimestamp": "2019-01-02T19:16:11.011Z"
  },
  "Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "IAM",
    "LastName": "IAM",
    "RoutingProfile": {
      "DefaultOutboundQueue": {
        "Name": "BasicQueue"
      },
      "InboundQueues": [
        "Name": "BasicQueue"
      }
    ],
    "Username": "agentUserName"
  },
  "Contacts": []
},

**Set up recording behavior**

Managers can monitor live conversations, and review and download recordings of past agent conversations. To set this up, you need to add the [Set recording and analytics behavior](#) block to
your flows, assign managers the appropriate permissions, and show them how to monitor live conversations and access past recordings in Amazon Connect.

**When is a conversation recorded?**

- The call recording feature has options for choosing whether to record the agent only, customer only, or agent and customer conversations.
- A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the flow.
- When call recording is enabled, the recording begins when the call is connected to an agent and stops when the agent disconnects.
- When a customer is on hold, the agent is still recorded.
- The transfer conversation between agents is recorded.
- Any transfers to external numbers are not recorded after the agent leaves the call.
- If the agent mutes their own microphone, for example, to consult with a coworker sitting next to them, their side-bar conversation is not recorded. The customer is still recorded since their microphone hasn't been muted.

**Where are recordings and transcripts stored?**

Agents and contacts are stored on separate, stereo audio channels.

- The agent audio is stored in the right channel.
- All incoming audio, including the customer and anyone conferenced in, is stored in the left channel.

Recordings are stored in the Amazon S3 bucket that are [created for your instance](#). Any user or application with the appropriate permissions can access the recordings in the Amazon S3 bucket.

Encryption is enabled by default for all call recordings using Amazon S3 server-side encryption with KMS. The encryption is at the object level. The reports and recording objects are encrypted; there's no encryption at the bucket level.

You shouldn't disable encryption.
Important

- For voice conversations to be stored in an Amazon S3 bucket, you need to enable recording in the flow block using the Set recording and analytics behavior block.
- For chat conversations, if there's an S3 bucket for storing chat transcripts, then all chats are recorded and stored there. If no bucket exists, then no chats are recorded. However, if you want to monitor chat conversations, you still need to add the Set recording and analytics behavior block to the flow.

Tip

We recommend using the contact ID to search for recordings. Even though many call recordings for specific contact IDs may be named with the contact ID prefix itself (for example, 123456-aaaa-bbbb-3223-2323234.wav), there is no guarantee that the contact IDs and name of the contact recording file always match. By using Contact ID for your search on the Contact search page, you can find the correct recording by referring the audio file on the contact record.

When are recordings available?

When call recording is enabled, the recording is placed in your S3 bucket shortly after the contact is disconnected. Then you can review the recording.

Important

You can also access the recording from the customer's contact record. The recording is available in the contact record, however, only after the contact has left the After Contact Work (ACW) state.

Tip

Amazon Connect uses the Amazon S3 PutObject and MultipartUpload APIs to upload the call recording to your S3 bucket. If you are using S3 Event Notifications when call recordings are uploaded successfully to your bucket, make sure you enable...
the notification for **All object create events**, or for both `s3:ObjectCreated:Put` and `s3:ObjectCreated:CompleteMultipartUpload` event types.

**Headset requirements for listening to recordings**

You need to use an output device (headset or other device) that supports stereo output so you can hear both the agent and customer audio.

Agent and customer recordings are presented in two separate channels. With a full headset, each side will play one channel. But for a one-ear headset, there isn't a mechanism to mix two channels into one.

**How to set up recording behavior**

To view a sample flow with the **Set recording behavior** block configured, see [Sample recording behavior](#).

**To set up recording behavior in your flows**

1. Log in to your Amazon Connect instance using an account that has permissions to edit flows.
2. On the navigation menu, choose **Routing, Contact flows**.
3. Open the flow that handles customer contacts you want to monitor.
4. In the flow, before the contact is connected to an agent, add a **Set recording and analytics behavior** block to the contact flow.
5. To configure the Set recording and analytics behavior block, choose from the following:

- To record voice conversations, choose what you want to record: **Agent and Customer, Agent only**, or **Customer only**.
- To record chat conversations, you need to choose **Agent and Customer**.
- To enable monitoring of voice and/or chat conversations, you need to choose **Agent and Customer**.

6. Choose Save and then Publish to publish the updated flow.

**To set up recording behavior for outbound calls**

1. Create a flow, using the outbound whisper flow type.
2. Add a Set recording and analytics behavior block to that contact flow.
3. Set up a queue that will be used for making outbound calls. In the Outbound whisper flow box, choose the flow that has Set recording and analytics behavior in it.

**How to set up users to monitor conversations or review recordings**

To learn what permissions managers need, and how they can monitor live conversations and review recordings of past conversations, see:

- Set up live monitoring for voice and/or chat
- Review recorded conversations between agents and customers using Amazon Connect

**How to set up S3 Object Lock for immutable call recordings**

You can use Amazon S3 Object Lock in combination with your call recording bucket to help prevent call recordings from being deleted or overwritten for a fixed amount of time, or indefinitely.

Object Lock adds another layer of protection against object changes and deletion. It can also help meet regulatory requirements for Write-Once-Read-Many (WORM) storage.

**Important things to know**

- You can enable Amazon S3 Object Lock only on new buckets. To configure it on an existing call recording bucket, contact AWS Support.
• Versioning must be enabled on your call recording bucket.

• After Amazon S3 Object Lock is enabled it cannot be removed.

• We recommend using a dedicated call recording bucket because all objects will be locked after the default Object Lock retention policy is applied.

• Ensure that your retention policy is appropriate for your requirements. After the policy is configured, your call recordings will be protected from deletion for the duration specified.

• We highly recommended you thoroughly test the policy in a non-production environment before implementing it in production.

Step 1: Create a new S3 bucket with Object Lock enabled

For a tutorial on creating a new S3 bucket with Object Lock enabled, see Protect Data on Amazon S3 Against Accidental Deletion or Application Bugs Using S3 Versioning, S3 Object Lock, and S3 Replication.

To enable Object Lock on an existing bucket, open an AWS Support ticket.

Step 2: Configure Amazon Connect to use the new S3 bucket for call recordings

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias.

3. In the navigation pane, choose Data storage.

4. In the Call recordings section, choose Edit.

5. Choose Select an existing S3 bucket, and then in the Name dropdown box choose the new Object Lock bucket.

6. Choose Save.
Step 3: Test Object Lock is enabled

1. Make a test call to your contact center to generate a call recording.

2. Log in to Amazon Connect at https://your-instance.my.connect.aws/home, with an Admin account, or an account that has permissions to search for contacts.

3. Choose Analytics and optimization, Contact search. Search for your call recording to find the contact ID. Copy the contact ID. You're going to use it in the next step to locate the call recording in your S3 bucket.

4. Open the Amazon S3 console, select the bucket you created in Step 1, and follow the path prefix. The path to the call recording includes the year, month, and day the recording was made. After you're in the correct path prefix, search for the contact ID of the call recording.

5. Select the Show versions toggle next to the Search box. This option allows you to attempt to delete the object instead of only applying a delete marker. Applying a delete marker is the standard behavior when you delete an object from an S3 bucket with versioning enabled.

6. Select the call recording (the box to the left of the recording name), and then choose Delete. In the confirmation box, type permanently delete and select Delete objects.

7. Review the Delete objects: status notification to confirm that the delete operation has been blocked due to the Object Lock policy.
Set up queued callback by creating flows, queues, and routing profiles

You can create flows that provide the ability for customers to leave their phone number and get a callback from an agent.

Contents

- Steps to set up queued callback
- The routing process
- How queued callbacks affect queue limits
- Create a flow for queued callbacks
- Learn more about queued callbacks

Steps to set up queued callback

Use the steps provided in the following overview to set up queued callback.

- **Set up a queue** specifically for callbacks. In your real-time metrics reports, you can look at that queue and see how many customers are waiting for callbacks.
- **Set up caller ID**. When setting your callback queue, specify the caller ID name and phone number that appears to customers when you call back.
• **Add the callback queue to a routing profile.** Set this up so that contacts waiting for a call are routed to agents.

• **Create a flow for queued callbacks.** You offer the option for a callback to the customer.

• **Associate a phone number with the inbound flow.**

• (Optional) Create an outbound whisper flow. When a queued call is placed, the customer hears this message after they pick up and before they connect to the agent. For example, "Hello, this is your scheduled callback..."

• (Optional) Create an agent whisper flow. This is what the agent hears right after they accept the contact, before they are joined to the customer. For example, "You're about to be connected to Customer John, who requested a refund for..."

### The routing process

1. When a customer leaves their number it's put in a queue and then routed to the next available agent.

2. After an agent accepts the callback in the CCP, Amazon Connect calls the customer.

   If no agents are available to work on callbacks, the callbacks can stay in queue for up to 7 days after they are created before Amazon Connect automatically removes them.

   **Tip**

   To manually remove a callback from the queue, use the [StopContact API](https://docs.aws.amazon.com/connect/latest/api/API_StopContact.html).

3. If there is no answer when the Amazon Connect calls the customer, it retries based on the number of times you've specified.

4. If the call goes to **voicemail**, it's considered connected.

5. If the customer calls again while in the callback queue, it's treated as a new call and will be handled as usual. To avoid duplicate callback requests in a callback queue, see this blog: [Preventing duplicate callback requests in Amazon Connect](https://docs.aws.amazon.com/connect/latest/userguide/call-via-queue.html).
How queued callbacks affect queue limits

- Queued callbacks count towards the queue size limit, but they are routed to the error branch. For example, if you have a queue that handles callbacks and incoming calls, and that queue reaches the size limit:
  - The next callback is routed to the error branch.
  - The next incoming call gets a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.
- Consider setting up your queued callbacks to be lower priority than your queue for incoming calls. This way, your agents only work on queued callbacks when the incoming call volume is low.

Create a flow for queued callbacks

To see what a flow looks like with queued callback, in new Amazon Connect instances see Sample queue configurations. In previous instances, see Sample queued callback.

The following procedure shows how to:

- Request a callback number from a customer.
- Store the callback number in an attribute.
- Reference the attribute in a Set callback number block to set the number to dial the customer.
- Transfer the customer to the callback queue.

At the basic level, here's what this queued callback flow looks like, without any of the alternative branches or error handling configured. The following image shows a flow with the following blocks: Get customer input, Store customer input, Set callback number, Play prompt, Transfer to queue, and Disconnect/hang up.
Following are the steps to create this flow.

**To create a flow for queued callbacks**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. Select an existing flow, or choose **Create flow** to create a new one.

   ![Tip]
   You can create this flow using different flow types: Customer queue flow, Transfer to agent, Transfer to queue.

3. Add a **Get customer input** block.
4. Configure the block to prompt the customer for a callback. The following image shows a message in the **Text-to-speech** box: **Press 1 to receive a callback. Press 2 to stay in queue**.

5. At the bottom of the block, choose **Add another condition**, and add options 1 and 2, as shown in the following image.
6. Add a **Store customer input** block.

7. Configure the block to prompt customers for their callback number, such as "Please enter your phone number." The following image shows the **Properties** page of the **Store customer input** block.

8. In the **Customer input** section, select **Phone number**, and then choose one of the following:

   - **Local format**: Your customers are calling from phone numbers that are in the same country as the AWS Region where you created your Amazon Connect instance.

   - **International format/Enforce E.164**: Your customers are calling from phone numbers in countries or regions other than the one where you created your instance.

9. Add a **Set callback number** block to your flow.

10. Configure the block to set **Type** to **System**, as shown in the following image. For **Attribute**, choose **Store customer input**. This attribute stores the customer's phone number.
11. Add a **Transfer to queue** block.

12. In the **Transfer to queue** block, configure the **Transfer to callback queue** tab as shown in the following image. Set **Initial delay** to 99. Set **Max number of retries** to 2. Set **Minimum time between attempts** to 10 minutes.

The following properties are available:
• **Initial delay**: Specify how much time has to pass between a callback contact being initiated in the flow, and the customer is put in queue for the next available agent. In the previous example, the time is 99 seconds.

• **Maximum number of retries**: If this is set to 2, then Amazon Connect tries to call back the customer a maximum of three times: the initial callback, and two retries.

A retry only happens if it rings but there's no answer. If the callback goes to voicemail, it's considered connected and Amazon Connect does not retry again.

---

**Tip**

We strongly recommend that you double-check the number entered in **Maximum number of retries**. If you accidentally enter a high number, such as 20, it's going to result in unnecessary work for the agent and too many calls for the customer.

---

• **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait until trying again. In the previous example, we wait 10 minutes between attempts.

13. In the **Optional parameters** section, choose **Set working queue** if you want to transfer the contact to a queue that you set up specifically for callbacks. This option is shown in the following image.

```
Optional parameters:

- Set working queue
  - By queue
    - Select a queue
      - Callback Queue
  - Use attribute
  - By agent
```

Creating a queue just for callbacks lets you view in your real-time metrics reports how many customers are waiting for callbacks.
If you don't set a working queue, Amazon Connect uses the queue that was set previously in the flow.

14. To save and test this flow, configure the other branches and add error handling. To see an example of how this is done, see Sample queue configurations. For previous instances, see Sample queued callback.

15. For information about how callbacks appear in real-time metrics reports and contact records, see About queued callbacks in metrics.

Learn more about queued callbacks

See the following topics to learn more about queued callbacks:

- About queued callbacks in metrics
- How Initial delay affects Scheduled and In queue metrics
- What counts as a "Failed Callback Attempt"
- Example: Metrics for a queued callback

Import/export flows

Use the procedures described in this topic to import/export a flows from the previous flow designer to the new one, from one instance to another, or from one Region to another as you expand your customer service organization.

Note

To copy and paste flows and blocks in the updated flow designer, the flow must be in the new flow language. To convert a legacy flow into the new format, you have two options:

- Option 1: In the flow designer, opt in to the updated flow designer. Your legacy flows are automatically converted.
- Option 2: Manually import the legacy flow using the updated flow designer.

This option is most useful for scenarios where you have stored your flows in JSON offline. For example, for configuration control, you may have flow configurations in an offline data store. To copy a part of that flow and paste it into the updated flow designer, you need to import it into the updated flow designer. The importing process converts it...
To the new flow language. After that, you can copy and paste within the updated flow designer. If you want to keep using your offline data store as a source of truth, update the flow with the new format.

To migrate tens or hundreds of flows, use the APIs described in Migrate flows to a different instance.

The Flow Import/Export feature is currently in Beta status. Updates and improvements that we make could result in issues in future releases importing flows that are exported during the beta phase.

Export limitations

You can export flows that meet the following requirements:

- The flow has fewer than 100 blocks.
- The total size of the flow is less than 1MB.

We recommend dividing large flows in to smaller ones to meet these requirements.

Flows are exported to JSON files

A flow is exported to a JSON file. It has the following characteristics:

- The JSON includes a section for each block in the flow.
- The name used for a specific block, parameter, or other element of the flow may be different than the label used for it in the flow designer.

By default, flow export files are created without a file name extension, and saved to the default location set for your browser. We suggest saving your exported flows to folder that contains only exported flows.

How to import/export flows

To export a flow

1. Log in to your Amazon Connect instance using an account that is assigned a security profile that includes view permissions for flows.
2. Choose **Routing, Contact flows**.
3. Open the flow to export.
4. Choose **Save, Export flow**.
5. Provide a name for the exported file, and choose **Export**.

**To import a flow**

1. Log in to your Amazon Connect instance. The account must be assigned a security profile that includes edit permissions for flows.
2. On the navigation menu, choose **Routing, Contact flows**.
3. Do one of the following:
   - To replace an existing flow with the one you are importing, open the flow to replace.
   - Create a new flow of the same type as the one you are importing.
4. Choose **Save, Import flow**.
5. Select the file to import, and choose **Import**. When the flow is imported into an existing flow, the name of the existing flow is updated, too.
6. Review and update any resolved or unresolved references as necessary.
7. To save the imported flow, choose **Save**. To publish, choose **Save and Publish**.

**Resolve resources in imported contact flows**

When you create a flow, the resources you include in the flow, such as queues and voice prompts, are referenced within the flow using the name of the resource and the Amazon Resource Name (ARN). The ARN is a unique identifier for a resource that is specific to the service and Region in which the resource is created. When you export a flow, the name and ARN for each resource referenced in the flow is included in the exported flow.

When you import a flow, Amazon Connect attempts to resolve the references to the Amazon Connect resources used in the flow, such as queues, by using the ARN for the resource.

- When you import a flow into the same Amazon Connect instance that you exported it from, the resources used in the flow will resolve to the existing resources in that instance.
- If you delete a resource, or change the permissions for a resource, Amazon Connect may not be able to resolve the resource when you import the flow.
• When a resource cannot be found using the ARN, Amazon Connect attempts to resolve the resource by finding a resource with the same name as the one used in the flow. If no resource with the same name is found, a warning is displayed on the block that contains a reference to the unresolved resource.

• If you import a flow into a different Amazon Connect instance than the one it was exported from, the ARNs for the resources used are different.

• If you create resources in the instance with the same name as the resource in the instance where the flow was exported from, the resources can be resolved by name.

You can also open the blocks that contain unresolved resources, or resources that were resolved by name, and change the resource to another one in the Amazon Connect instance.

You can save a flow with unresolved or missing resources. You can publish a flow with unresolved or missing resources only for optional parameters. If any required parameter has an unresolved resource, you cannot publish the flow until the resources are resolved.

Add an Amazon Lex bot to Amazon Connect

In this article we guide you through the steps to add an Amazon Lex bot to Amazon Connect.

With Amazon Lex, you can build conversational interactions (bots) that feel natural to your customers. Amazon Connect with Amazon Lex bots can also capture customer input as digits that customers enter on their numeric keypad when used in an Amazon Connect flow. This way customers can choose how they want to enter sensitive information such as account numbers.

To follow along with this walkthrough, you need the following:

• An active AWS account.
• An Amazon Connect instance.

Tip
You can also use Amazon Lex to power interactive messages for Amazon Connect chat. Interactive messages are rich messages that present a prompt and pre-configured display options that a customer can select from. These messages are powered by Amazon Lex and
Create an Amazon Lex bot

In this step you'll create a custom bot to demonstrate the Press or Say integration with Amazon Connect. The bot prompts callers to press or say a number that matches the menu option for the task to complete. In this case, the input is checking their account balance.

Amazon Lex

1. Open the Amazon Lex console.
2. Choose Create bot.
3. On the Configure bot settings page, choose Create - Create a blank bot and provide the following information:
   - Bot name — For this walkthrough, name the bot AccountBalance.
   - IAM permissions — Select a role if you have one created. Otherwise, choose Create a role with basic Amazon Lex permissions.
   - COPPA — Choose whether the bot is subject to the Child Online Privacy Protection Act.
   - Session timeout — Choose how long the bot should wait to get input from a caller before ending the session.
4. Choose Next.
5. Provide language and voice specific information:
   - Language — Select language and locale from the list of Languages and locales supported by Amazon Lex.
   - Voice interaction — Select the voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joanna.
6. Choose Done. The AccountBalance bot is created, and the Intent page is displayed.

Amazon Lex (Classic)

1. Open the Amazon Lex console.
2. If you are creating your first bot, choose Get Started. Otherwise, choose Bots, Create.
3. On the Create your bot page, choose Custom bot and provide the following information:

- **Bot name** — For this walkthrough, name the bot AccountBalance.
- **Output voice** — Select the voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joanna.
- **Session timeout** — Choose how long the bot should wait to get input from a caller before ending the session.
- **COPPA** — Choose whether the bot is subject to the Child Online Privacy Protection Act.

4. Choose Create.

### Configure the Amazon Lex bot

In this step you'll determine how the bot responds to customers by providing intents, sample utterances, slots for input, and error handling.

For this example, you'll configure the bot with two intents: one to look up account information, and another to speak with an agent.

#### Create AccountLookup intent

Amazon Lex

1. After you created the bot, you are on the Intents page the Amazon Lex console. If you're not there, you can get there by choosing Bots, AccountBalance, Bot versions, Draft version, Intents. Choose Add intent, Add empty intent.

2. In the Intent name box, enter AccountLookup.

3. Scroll down the page to Sample utterances. In this step you enter utterances that allow the customer to elicit the AccountLookup intent. Enter the following utterances, and choose Add utterance after each one.

   - **Check my account balance**
   - **One**: This assigns the utterance of "one" or key press of "1" to the AccountLookup intent.

The following image shows where to add the utterance in the Sample utterances section.
4. Scroll to the **Slots** section, and choose **Add slot**. Complete the box as follows:

   a. **Required for this intent** = selected.
   
   b. **Name** = **AccountNumber**.
   
   c. **Slot type** = **AMAZON.Number**.
   
   d. **Prompts** = the text to be spoken when the call is answered. For example, ask callers to enter their account number using their keypad: **Using your touch-tone keypad, please enter your account number**. Choose **Add**.

The following image shows a completed **Add slot** section.
5. Scroll to the **Closing responses** section. Add a message for the bot to say to customers. For example, **Your account balance is $1,234.56.** (For this walkthrough, we aren't going to actually get the data, which is what you would do in reality.)

   The following image shows a completed **Closing responses** section.
6. Choose **Save intent**.

Amazon Lex (Classic)

1. In the Amazon Lex console choose the + icon next to **Intents**, and choose **Create new intent**.
2. Name the intent **AccountLookup**.
3. Add a sample utterance, such as **Check my account balance**, and choose the + icon.
4. Add a second utterance, such as **One** and choose the + icon. This assigns the utterance of "one" or key press of "1" to the **AccountLookup** intent.

**Tip**

You must add an utterance of "one" in the bot, and not the number "1". This is because Amazon Lex doesn't support numeric input directly. To get around this,
5. Under **Slots**, add a slot named **AccountNumber**.

The following image shows the location of the **Slots** section on the page.

![Image of Slots section](image)

6. For **Slot type**, use the drop-down to choose **AMAZON.NUMBER**.

7. For **Prompt**, add the text to be spoken when the call is answered. For example, ask callers to enter their account number using their keypad: *Using your touch-tone keypad, please enter your account number.*

8. Choose the + icon.

9. Make sure that the **Required** check box is selected.

10. In the **Response** section, add a message for the bot to say to customers. For example, *Your account balance is $1,234.56.*

11. Choose **Save Intent**.

**Create SpeakToAgent intent**

Amazon Lex

1. Navigate to the **Intents** page: choose **Back to intents list**.
2. Choose **Add intent, Add empty intent**.
3. In the **Intent name** box, enter **SpeakToAgent**, and then choose **Add**.
4. Scroll down to **Sample utterances** section. Enter the following utterances, which allow the customer to elicit the SpeakToAgent intent:
   - **Speak to an agent**
   - **Two**
5. Scroll down to the **Closing responses** section. Add a message for the bot to say to customers. For example, **Okay, an agent will be with you shortly**.
6. Choose **Save intent**.

**Amazon Lex (Classic)**
1. In the Amazon Lex console choose the + icon next to **Intents**, and choose **Create new intent**.
2. Name the intent **SpeakToAgent**.
3. Select **SpeakToAgent**.
4. Add a sample utterance, such as **Speak to an agent**, and choose +.
5. Add a second utterance, such as **Two**, and choose +.
6. Add a message that lets callers know that their call is being connected to an agent. For example, "Okay, an agent will be with you shortly."
7. Choose **Save Intent**.

**Build and test the Amazon Lex bot**

After you create your bot, make sure it works as intended.

**Amazon Lex**
1. At the bottom of the page, choose **Build**. It may take a minute or two. The following image shows where the **Build** button is located.
2. When it's finished building, choose **Test**.

3. Let's test the **AccountLookup** intent: In the **Test Draft version** pane, in the **Type a message** box, type 1 and press Enter. Then type a fictitious account number and press Enter. The following image shows where you enter intent.

   a. Clear the test box.
   b. Type the intents you want to test.

4. To confirm that the **SpeakToAgent** intent is working, clear the test box, and then type 2 and press Enter. The following image shows what the test looks like after you clear it and then enter 2.
5. Close the **Test Draft version** pane.

Amazon Lex (Classic)

1. Choose **Build**. It may take a minute or two.

2. When it's finished building, choose **Test Chatbot**, as shown in the following image.

3. Let's test the **AccountLookup** intent: In the **Test Chatbot** pane, in the **Chat with your bot** box, type 1. Then type a fictitious account number. In the following image, the arrow points to the box where you type 1.
4. Choose Clear chat history.

5. To confirm that the SpeakToAgent intent is working, type 2.

Create a bot version (Optional)

In this step you create a new bot version to use in an alias. It’s how you create an alias that can be used in a production environment. Test aliases are subject to lower throttling limits. Although this is a test walkthrough, creating a version is a best practice.

Amazon Lex

1. If you're on the Intents page, choose Back to intents list.
2. On the left menu, choose Bot versions.
3. Choose Create version.
4. Review the details of the AccountBalance bot, and then choose Create.

This creates a version of your bot (Version 1). You can switch versions on an non-test alias without having to track which version is getting published.
Create an alias for the bot

Amazon Lex

1. In the left menu, choose **Aliases**.
2. On the **Aliases** page, choose **Create alias**.
3. In the **Alias name** box, enter a name, such as **Test**. Later in this walkthrough you'll use this alias to specify this version of the bot in your flow.

   > **Important**
   
   In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see **Runtime quotas**.

4. For **Associated version**, choose the version you just created, such as **Version 1**.
5. Choose **Create**.
1. Choose **Publish**.

2. Provide an alias for your bot. Use the alias to specify this version of the bot in the flow, for example, **Test**.

   **Important**
   
   In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see [Runtime Service Quotas](#).

3. Choose **Publish**.

### Add the Amazon Lex bot to your Amazon Connect instance

**Amazon Lex**

1. Open the [Amazon Connect console](#).

2. Select the Amazon Connect instance that you want to integrate with your Amazon Lex bot.

   ![Amazon Connect instance](#)

3. On the navigation menu, choose **Contact flows**.

4. Under **Amazon Lex**, use the dropdown to select the Region of your Amazon Lex bot, and then select your Amazon Lex bot, **AccountBalance**.

5. Select the Amazon Lex bot alias name from the dropdown (**Test**), and then choose **+ Add Lex Bot**. The following image shows Amazon Lex section after it has been configured.
Amazon Connect uses Amazon Lex resource-based policies to make calls to your Amazon Lex bot. When you associate an Amazon Lex bot with your Amazon Connect instance, the resource-based policy on the bot is updated to give Amazon Connect permission to invoke the bot. For more information on Amazon Lex resource-based policies, see How Amazon Lex works with IAM.

Amazon Lex (Classic)

1. Open the Amazon Connect console.
2. Select the Amazon Connect instance that you want to integrate with your Amazon Lex bot.
3. On the navigation menu, choose Contact flows.
4. Under **Amazon Lex**, select the Region of your Amazon Lex classic bot from the dropdown, and then select your Amazon Lex classic bot. It’s name will have the suffix "(Classic)". Then choose **Add Lex Bot**.

### Create a flow and add your Amazon Lex bot

⚠️ **Important**

If you're using an Amazon Lex V2 bot, your language attribute in Amazon Connect must match the language model used to build your Lex bot. This is different than Amazon Lex (Classic). Use a **Set voice** block to indicate the Amazon Connect language model, or use a **Set contact attributes** block.

Next, create a new flow that uses your Amazon Lex bot. When you create the flow, you configure the message played to callers.

1. Log in to your Amazon Connect instance with an account that has permissions for contact flows and Amazon Lex bots.
3. Under **Interact**, drag a **Get customer input** block onto the designer, and connect it to the **Entry point block**.
4. Choose the **Get customer input** block to open it. Choose **Text to speech or chat text, Enter text**.
5. Type a message that provides callers with information about what they can do. For example, use a message that matches the intents used in the bot, such as "To check your account balance, press or say 1. To speak to an agent, press or say 2." The following image shows this message on the Properties page of the **Get customer input** block.
6. Select the **Amazon Lex** tab, as shown in the following image.
7. In the **Name** dropdown, select the **AccountBalance** bot you created earlier.

   a. If you selected an Amazon Lex bot, under **Alias** use the dropdown menu to select the bot alias, **Test**.

   b. Amazon Lex Classic bots have the suffix "(Classic)" appended to their names. If you have selected a Classic bot, enter the alias you want to use in the **Alias** field.

   c. For Amazon Lex V2 bots, you also have the option of manually setting a bot alias ARN. Choose **Set manually**, then either type the ARN of the bot alias you want to use or set the ARN using a dynamic attribute.

8. Under **Intents**, choose **Add an intent**.

9. Type **AccountLookup** and choose **Add another intent**. The following image shows the **Intents** section configured with this information.
10. Type **SpeakToAgent** and choose **Save**.

**Finish the flow**

In this step you finish adding parts to the flow that run after the caller interacts with the bot:

1. If the caller presses 1 to get their account balance, use a **Prompt** block to play a message and disconnect the call.
2. If the caller presses 2 to speak to an agent, use a **Set queue** block to set the queue and transfer the caller to the queue, which ends the flow.

Here are the steps to create the flow:

1. Under **Interact**, drag a **Play prompt block** to the designer, and connect the **AccountLookup** node of the **Get customer input** block to it. After the customer gets their account balance from the Amazon Lex bot, the message in the **Play prompt** block plays.
2. Under **Terminate/Transfer**, drag a **Disconnect** block to the designer, and connect the **Play prompt** block to it. After the prompt message plays, the call is disconnected.

To complete the **SpeakToAgent** intent:

1. Add a **Set working queue** block and connect it to the **SpeakToAgent** node of the **Get customer input** block.
2. Add a **Transfer to queue** block.
3. Connect the Success node of the **Set customer queue flow** block to the **Transfer queue**.
4. Choose **Save**, then **Publish**.
Your finished flow will look something like the following image. The flow starts with the **Get customer input** block. That block branches to **Play prompt** or **Set customer queue**.

1. Open the Amazon Connect console.
2. Choose **Routing, Phone numbers**.
3. On the **Manage Phone numbers** page, select the phone number to assign to the flow.
4. Add a description.
5. In the **Flow/IVR** menu, choose the flow that you just created.
6. Choose **Save**.

---

**Tip**

If your business uses multiple locales in a single bot, add a **Set contact attributes** block to the beginning of your flow. Configure this block to use the `$.LanguageCode` system attribute.

---

### Assign the flow to a phone number

When customers call in to your contact center, the flow to which they are sent is the one assigned to the telephone number that they called. To make the new flow active, assign it to a phone number for your instance.

1. Open the Amazon Connect console.
2. Choose **Routing, Phone numbers**.
3. On the **Manage Phone numbers** page, select the phone number to assign to the flow.
4. Add a description.
5. In the **Flow/IVR** menu, choose the flow that you just created.
6. Choose **Save**.
Try it!

To try the bot and flow, call the number you assigned to the flow. Follow the prompts.

Add interactive messages to chat

Interactive messages are rich messages that present a prompt and pre-configured display options for a customer to choose. These messages are powered by Amazon Lex and configured through Amazon Lex using a Lambda.

Tip

If you have integrated with Apple Messages for Business, see Interactive Message Types on the Apple website.

Validation limits

The string field limits (for example, title, subtitle, etc.) are expected to be enforced by the client (that is, a custom built interface or the hosted communications widget). The SendMessage API checks only that the total size of the string is less than 20KB.

- When you use the hosted communications widget without customizing it, if the string exceeds field limits, it is truncated on the user interface and an ellipsis (...) is appended. You can determine how to enforce field limits by customizing the widget.
- If you are integrating with other platforms (such as Apple Messages for Business), review the limits in this topic for Amazon Connect, and review the limits in the documentation for the other platform. For example, quick replies are not supported on older versions of iOS.

All other field limits must be followed for the message to be successfully sent.

Message display templates

Amazon Connect provides the following message display templates for you to use to render information to customers in a chat:

- List picker
- Time picker
- Panel
These templates define how the information is going to render, and what information is surfaced in the chat interface. When interactive messages are sent through chat, flows validate that the message format follows one of these templates.

**List picker template**

Use the list picker template to present the customer with a list of up to six choices. Each choice can have its own image.

The following images show two examples of how the list picker template renders information in a chat.

- One image shows three buttons, each one with the name of a fruit in text: apple, orange, banana.
- The second image shows a picture of a store and then under it, three buttons, each one with the name, image, and price of the fruit.
The following code is the list picker template that you can use in your Lambda. Note the following:

- **Bold text** is a mandatory parameter.
- In some cases, if the parent element exists in the request and it isn't mandatory/bold, but the fields in it are, then the fields are mandatory. For example, see `data.replyMessage` structure in the following template. If the structure exists, title is mandatory. Otherwise complete `replyMessage` is optional.

```json
{
   "templateType": "ListPicker",
   "version": "1.0",
   "data": {
      "replyMessage": {
         "title": "Thanks for selecting!",
         "subtitle": "Produce selected",
         "imageType": "URL",
         "imageData": "https://interactive-msg.s3-us-west-2.amazonaws.com/fruit_34.3kb.jpg",
         "imageDescription": "Select a produce to buy"
      },
      "content": {
         "title": "What produce would you like to buy?",
         "subtitle": "Tap to select option",
         "imageType": "URL",
         "imageData": "https://interactive-msg.s3-us-west-2.amazonaws.com/fruit_34.3kb.jpg",
         "imageDescription": "Select a produce to buy",
         "elements": [
            {
               "title": "Apple",
               "subtitle": "$1.00",
               "imageType": "URL",
               "imageData": "https://interactive-message-testing.s3-us-west-2.amazonaws.com/apple_4.2kb.jpg"
            },
            {
               "title": "Orange",
               "subtitle": "$1.50",
               "imageType": "URL",
               "imageData": "https://interactive-message-testing.s3-us-west-2.amazonaws.com/orange_17.7kb.jpg"
            }
         ]
      }
   }
}
```
List picker limits

The following table lists the limits for each of the list picker elements, should you choose to build your own Lambda from scratch. The mandatory parameters are in bold.

To send unlimited options, implement action buttons in your application. For more information, see Implementation of action buttons in interactive message list picker/panel.

<table>
<thead>
<tr>
<th>Parent field</th>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>templateType</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Valid template type</td>
</tr>
<tr>
<td></td>
<td>data</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Must be &quot;1.0&quot;</td>
</tr>
<tr>
<td>data</td>
<td>content</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data</td>
<td>replyMessage</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>content title</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
<td>Should be a description for promptless templates</td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>elements</td>
<td>Yes</td>
<td>1 item</td>
<td>6 items</td>
<td>This is an array of elements. Maximum 6 elements in the array. To send unlimited elements, use the action buttons feature.</td>
</tr>
<tr>
<td></td>
<td>subtitle</td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>imageType</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Must be &quot;URL&quot;</td>
</tr>
<tr>
<td></td>
<td>imageData</td>
<td>No</td>
<td>0</td>
<td>200</td>
<td>Must be a valid publicly accessible URL</td>
</tr>
<tr>
<td></td>
<td>imageDesc</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>referenceId</td>
<td>No</td>
<td></td>
<td></td>
<td>String. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>listId</td>
<td>No</td>
<td></td>
<td></td>
<td>String. Only required for action button feature.</td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>preIndex</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>nextIndex</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>templateIdentifier</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Should be an UUID. <strong>This field is required</strong> if List Picker/Panel is being used in a Carousel.</td>
</tr>
<tr>
<td></td>
<td>elementsTitle</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subtitle</td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>imageType</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Must be &quot;URL&quot;</td>
</tr>
<tr>
<td></td>
<td>imageData</td>
<td>No</td>
<td>0</td>
<td>200</td>
<td>Must be a valid publicly accessible URL</td>
</tr>
<tr>
<td></td>
<td>imageDescription</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Cannot exist without an image</td>
</tr>
</tbody>
</table>
### Time picker template

The time picker template is useful for enabling customers to schedule appointments. You can provide up to 40 timeslots to the customer in a chat.

The following images show two examples of how the time picker template renders information in a chat.

- One image shows one date, and under it, one time slot.
- The second image shows one date, and under it, two time slots.

<table>
<thead>
<tr>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>actionDetail</td>
<td>No</td>
<td></td>
<td></td>
<td>Only required for action button feature. Must be &quot;PREVIOUS _OPTIONS&quot; or &quot;SHOW_MOR E&quot;.</td>
</tr>
<tr>
<td>replyMessage</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>subtitle</td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>imageType</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Must be &quot;URL&quot;</td>
</tr>
<tr>
<td>imageData</td>
<td>No</td>
<td>0</td>
<td>200</td>
<td>Must be a valid publicly accessible URL</td>
</tr>
<tr>
<td>imageDescription</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Cannot exist without an image</td>
</tr>
</tbody>
</table>
The following code is the time picker template that you can use in your Lambda. Note the following:

- **Bold text** is a mandatory parameter.
- In some cases, if the parent element exists in the request and it isn’t mandatory/bold, but the fields in it are, then the fields are mandatory. For example, see `data.replyMessage` structure in the following template. If the structure exists, title is mandatory. Otherwise complete `replyMessage` is optional.

```json
{
    "templateType":"TimePicker",
    "version":"1.0",
    "data":{
        "replyMessage":{
            "title":"Thanks for selecting",
            "subtitle":"Appointment selected",
        },
        "content":{
            "title":"Schedule appointment",
            "subtitle":"Tap to select option",
        }
    }
}
```
"timeZoneOffset": -450,
"location": {
   "latitude": 47.616299,
   "longitude": -122.4311,
   "title": "Oscar",
   "radius": 1,
},
"timeslots": [
   {
      "date": "2020-10-31T17:00+00:00",
      "duration": 60,
   },
   {
      "date": "2020-11-15T13:00+00:00",
      "duration": 60,
   },
   {
      "date": "2020-11-15T16:00+00:00",
      "duration": 60,
   }
],
}

Time picker limits

The following table lists the limits for each of the time picker elements. Use this information if you choose to build your own Lambda from scratch. The mandatory parameters are in bold.

<table>
<thead>
<tr>
<th>Parent field</th>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>templateType</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Valid template type</td>
</tr>
<tr>
<td></td>
<td>data</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Must be &quot;1.0&quot;</td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>data</td>
<td>replyMessage</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>content</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>replyMessage</td>
<td>title</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td>Should be description for promptless templates</td>
</tr>
<tr>
<td>subtitle</td>
<td></td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>content</td>
<td>title</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td>Should be description for promptless templates</td>
</tr>
<tr>
<td>subtitle</td>
<td></td>
<td>No</td>
<td>0</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>timezone offset</td>
<td>No</td>
<td>-720</td>
<td>840</td>
<td>This is an optional field when not set. Our sample client defaults to the user's timezone. If set, this displays per the timezone entered. The field should be an integer representing the number of minutes from GMT, specifying the timezone of the event's location.</td>
</tr>
<tr>
<td></td>
<td>location</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>timeslots</td>
<td>Yes</td>
<td>1</td>
<td>40</td>
<td>This is an array of timeslots. Maximum of 40 elements in the array.</td>
</tr>
<tr>
<td></td>
<td>longitude</td>
<td>Yes</td>
<td>-180</td>
<td>180</td>
<td>Must be double</td>
</tr>
<tr>
<td></td>
<td>latitude</td>
<td>Yes</td>
<td>-90</td>
<td>90</td>
<td>Must be double</td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>title</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>radius</td>
<td>No</td>
<td>0</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td></td>
<td>timeslotsdate</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Should be in ISO-8601 time format: YYYY-MM-DDTHH.MM+00.00 For example: &quot;2020-08-14T21:21+00.00&quot;</td>
</tr>
<tr>
<td></td>
<td>duration</td>
<td>Yes</td>
<td>1</td>
<td>3600</td>
<td></td>
</tr>
</tbody>
</table>

**Panel template**

By using the panel template, you can present the customer with up to 10 choices under one question. However, you can include only one image, rather than an image with each choice.

The follow image shows an example of how the panel template renders information in a chat. It shows an image at the top of the message, and under the image it shows a prompt that asks *How can I help? Tap to select option*. Under the prompt three options are displayed to the customer: **Check self-service options, Talk to an agent, End chat.**
The following code is the panel template that you can use in your Lambda. Note the following:

- **Bold text** is a mandatory parameter.
- In some cases, if the parent element exists in the request and it isn't mandatory/bold, but the fields in it are, then the fields are mandatory. For example, see `data.replyMessage` structure in the following template. If the structure exists, title is mandatory. Otherwise, complete `replyMessage` is optional.

```json
{
  "templateType": "Panel",
  "version": "1.0",
  "data": {
    "replyMessage": {
      "title": "Thanks for selecting!",
      "subtitle": "Option selected",
    },
    "content": {
      "title": "How can I help you?",
      "subtitle": "Tap to select option",
      "imageType": "URL",
      "imageData": "https://interactive-msg.s3-us-west-2.amazonaws.com/company.jpg",
      "imageDescription": "Select an option",
      "elements": [
        { "title": "Check self-service options",
        },
      ]
    }
  }
}
```
Panel limits

The following table lists the limits for each of the panel elements, should you choose to build your own Lambda from scratch. The mandatory parameters are in bold.

To send unlimited options, implement action buttons in your application. For more information, see Implementation of action buttons in interactive message list picker/panel.

<table>
<thead>
<tr>
<th>Parent field</th>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>templateType</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Valid template type</td>
</tr>
<tr>
<td></td>
<td>data</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Must be &quot;1.0&quot;</td>
</tr>
<tr>
<td></td>
<td>data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>replyMessage</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>content</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>content</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td>Should be a description for promptless templates</td>
</tr>
<tr>
<td></td>
<td>subtitle</td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>Parent field</td>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>elements</td>
<td>Yes</td>
<td>1 item</td>
<td>10 items</td>
<td>This is an array of elements. Maximum 10 elements in the array.</td>
</tr>
<tr>
<td></td>
<td>imageType</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Must be &quot;URL&quot;</td>
</tr>
<tr>
<td></td>
<td>imageData</td>
<td>No</td>
<td>0</td>
<td>200</td>
<td>Must be a valid publicly accessible URL</td>
</tr>
<tr>
<td></td>
<td>imageDescr</td>
<td>No</td>
<td>0</td>
<td>50</td>
<td>Cannot exist without an image</td>
</tr>
<tr>
<td></td>
<td>referencedId</td>
<td>No</td>
<td></td>
<td></td>
<td>String. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>listId</td>
<td>No</td>
<td></td>
<td></td>
<td>String. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>preIndex</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Only required for action button feature.</td>
</tr>
<tr>
<td></td>
<td>nextIndex</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Only required for action button feature.</td>
</tr>
</tbody>
</table>
### Quick reply template

Use quick reply messages to get simple responses from customers and them to customers in an in-line list. You can present customers with up to 5 options in one quick reply message. Images are not supported for quick replies.

The following image shows an example of how the quick reply template renders information in a chat.

<table>
<thead>
<tr>
<th>Parent field</th>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>templateIdentifier</td>
<td>No</td>
<td></td>
<td></td>
<td>Number. Should be an UUID. <strong>This field is required</strong> if List Picker/Panel is being used in a Carousel.</td>
</tr>
<tr>
<td></td>
<td>elements</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>title</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Only required for action button feature. Must be &quot;PREVIOUS_OPTIONS&quot; or &quot;SHOW_MORE&quot;.</td>
</tr>
<tr>
<td></td>
<td>actionDetail</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>replyMessage</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subtitle</td>
<td>No</td>
<td>0</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>
The following code is the quick reply template that you can use in your Lambda.

```json
{
    "templateType": "QuickReply",
    "version": "1.0",
    "data": {
        "content": {
            "title": "Which department would you like?",
            "elements": [
                {
                    "title": "Billing"
                },
                {
                    "title": "Cancellation"
                },
                {
                    "title": "New Service"
                }
            ]
        }
    }
}
```

**Quick reply limits**

The following table lists the limits for each of the quick reply elements. Use this information if you choose to build your own Lambda from scratch. The mandatory parameters are in bold.
<table>
<thead>
<tr>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateType</td>
<td></td>
<td></td>
<td></td>
<td>Valid template type</td>
</tr>
<tr>
<td>data</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>version</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Must be &quot;1.0&quot;</td>
</tr>
<tr>
<td>content</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>title</td>
<td>Yes</td>
<td>1</td>
<td>400</td>
<td>Should be a description for promptless templates</td>
</tr>
<tr>
<td>elements</td>
<td>Yes</td>
<td>2 item</td>
<td>5 items</td>
<td>This is an array of elements. Minimum 2 elements and maximum 5 elements in the array.</td>
</tr>
<tr>
<td>title</td>
<td>Yes</td>
<td>1</td>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>

**Carousel template**

Use carousels to display up to 5 list pickers or panels to customers in a single message. Similar to the list picker and time picker, you can add more options to the carousel by using the SHOW_MORE feature.

The following GIF shows an example of how the carousel template renders information in a chat. Customers scroll through the carousel of images by using the left and right arrows.
The following image shows two Learn More hyperlinks, which are examples of carousel picker hyperlink elements.

The following code is the carousel template that you can use in your Lambda.
"templateType": "Carousel",
"version": "1.0",
"data": {
  "content": {
    "title": "View our popular destinations",
    "elements": [
      {
        "templateIdentifier": "template0",
        "templateType": "Panel",
        "version": "1.0",
        "data": {
          "content": {
            "title": "California",
            "subtitle": "Tap to select option",
            "elements": [
              {
                "title": "Book flights"
              },
              {
                "title": "Book hotels"
              },
              {
                "title": "Talk to agent"
              }
            ]
          }
        }
      },
      {
        "templateIdentifier": "template1",
        "templateType": "Panel",
        "version": "1.0",
        "data": {
          "content": {
            "title": "New York",
            "subtitle": "Tap to select option",
            "elements": [
              {
                "title": "Book flights"
              },
              {
                "title": "Book hotels"
              }
            ]
          }
        }
      }
    ]
  }
}
}
For hosted communications widget users:

- The selections on the carousel template result in a JSON string response structured like the following example, to be sent back to Lambda (other interactive message types return regular string response with only selectionText value):

```json
{
    templateIdentifier: "template0",
    listTitle: "California",
    selectionText: "Book hotels"
}
```

- In carousels, you can provide hyperlinks in the list picker/panel elements. To create a hyperlink instead of a button, include the following additional fields for the element that should be a hyperlink:

```json
{
    title: "Book flights",
    ...  
    type: "hyperlink",
    url: "https://www.example.com/Flights"
}
```

**Carousel limits**

The following table lists the limits for each of the carousel elements. Use this information if you choose to build your own Lambda from scratch. The mandatory parameters are in bold.
<table>
<thead>
<tr>
<th>Parent field</th>
<th>Field</th>
<th>Required</th>
<th>Minimum characters</th>
<th>Maximum characters</th>
<th>Other requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>templateType</code></td>
<td>Yes</td>
<td></td>
<td></td>
<td>Valid template type</td>
</tr>
<tr>
<td></td>
<td><code>data</code></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>version</code></td>
<td>Yes</td>
<td></td>
<td></td>
<td>Must be &quot;1.0&quot;</td>
</tr>
<tr>
<td><code>data</code></td>
<td><code>content</code></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>content</code></td>
<td></td>
<td>1</td>
<td>400</td>
<td>Should be a description for promptless templates</td>
</tr>
<tr>
<td></td>
<td><code>elements</code></td>
<td>Yes</td>
<td>2 item</td>
<td>5 items</td>
<td>This is an array of either list pickers or panel templates. Only one interactive message type is accepted per carousel. Each element should include the top-level field <code>templateId</code>. Minimum 2 templates and maximum 5 templates in the array.</td>
</tr>
<tr>
<td>Field</td>
<td>Required</td>
<td>Minimum characters</td>
<td>Maximum characters</td>
<td>Other requirement</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>omitTitle FromCarouselResponse</td>
<td>No</td>
<td></td>
<td></td>
<td><strong>Note</strong> For the best customer experience, we recommend that each template has consistent use of images/number of elements.</td>
<td></td>
</tr>
</tbody>
</table>

**Boolean** - Optionally respond with "Selection Text" instead of the default "PickerTitle : Selection Text".
Rich formatting in titles and subtitles

You can add rich formatting to the titles and subtitles of your chat messages. For example, you can add links, italics, bold, numbered lists, and bulleted lists. You use markdown to format your text.

The following image of a chat box shows an example list picker with rich formatting in the title and subtitle.

- The title **How can we help? aws.amazon.com** is bold and contains a link.
- The subtitle contains italics and bold text, a bulleted list, and a numbered list. It also shows a plain link, text link, and sample code.
- The bottom of the chat box shows three list picker elements.
### How to format text with markdown

You can write title and subtitle strings in a multi-line format, or in a single line with `\r\n` line break characters.

- **Multi-line format**: The following code sample shows how to author lists in markdown in a multi-line format.

```javascript
const MultiLinePickerSubtitle = `This is some *emphasized text* and some **strongly emphasized text**
This is a bulleted list:
* item 1
* item 2
* item 3

This is a numbered list:
1. item 1
2. item 2
3. item 3
```

Questions? Visit [https://plainlink.com/faq](https://plainlink.com/faq)
3. item 3

Questions? Visit https://plainlink.com/faq

[This is a link](https://aws.amazon.com)

This is `\`
`

```
const PickerTemplate = {
    templateType: "ListPicker|Panel",
    version: "1.0",
    data: {
        content: {
            title: "How can we help?",
            subtitle: MultiLinePickerSubtitle,
            elements: [ /* ... */ ]
        }
    }
}
```

- **Single line format**: The following example shows how to author a subtitle in a single line by using `\r\n` line break characters.

```
const SingleLinePickerSubtitle = "This is some *emphasized text* and some **strongly emphasized text**\r\nThis is a bulleted list:\n* item 1\n* item 2\n* item 3\n
This is a numbered list:
1. item 1
2. item 2
3. item 3

Questions? Visit https://plainlink.com/faq\r\n[This is a link](https://aws.amazon.com)\r\nThis is `<code>`
```

```
const PickerTemplate = {
    templateType: "ListPicker|Panel",
    version: "1.0",
    data: {
        content: {
            title: "How can we help?",
            subtitle: SingleLinePickerSubtitle,
            elements: [ /* ... */ ]
        }
    }
}
```
This is some *emphasized text* and some **strongly emphasized text**

The following example shows how to format text as code with markdown:

This is `<code />`

**How to format links with markdown**

To create a link, use the following syntax:

[aws](https://aws.amazon.com)

The following examples show two ways you can add links with markdown:

Questions? Visit https://plainlink.com/faq

[This is a link](https://aws.amazon.com)

You can also set the target attribute of a link by using rehype syntax (default is `target="_blank"`). For example:

[plain text](https://example.com)<!--rehype:target=_self-->

**Invoke AWS Lambda functions**

Amazon Connect can interact with your own systems and take different paths in flows dynamically. To achieve this, invoke AWS Lambda functions in a flow, fetch the results, and call your own services or interact with other AWS data stores or services. For more information, see the [AWS Lambda Developer Guide](https://aws.amazon.com/)

To invoke a Lambda function from a flow, complete the following tasks.

**Tasks**

- [Create a Lambda function](https://aws.amazon.com/)
- [Add a Lambda function to your Amazon Connect instance](https://aws.amazon.com/)
- [Invoke a Lambda function from a flow](https://aws.amazon.com/)
- [Configure your Lambda function to parse the event](https://aws.amazon.com/)
- [Verify the function response](https://aws.amazon.com/)
Create a Lambda function

Create a Lambda function, using any runtime, and configure it. For more information, see Get started with Lambda in the AWS Lambda Developer Guide.

If you create the Lambda function in the same Region as your contact center, you can use the Amazon Connect console to add the Lambda function to your instance as described in the next task, Add a Lambda function to your Amazon Connect instance. This automatically adds resource permissions that allow Amazon Connect to invoke the Lambda function. Otherwise, if the Lambda function is in a different Region, you can add it to your flow using the flow designer and add the resource permissions using the add-permission command, with a principal of connect.amazonaws.com and the ARN of your Amazon Connect instance. For more information, see Using Resource-Based Policies for AWS Lambda in the AWS Lambda Developer Guide.

Add a Lambda function to your Amazon Connect instance

Before you can use an Lambda function in a flow, you need to add it to your Amazon Connect instance.

Add a Lambda function to your instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose your instance name in the Instance Alias column. This instance name appears in the URL you use to access Amazon Connect.

3. In the navigation pane, choose Flows.
4. In the AWS Lambda section, use the Function drop-down box to select the function to add to your instance.

Tip
The drop-down lists only those functions in the same Region as your instance. If no functions are listed, choose Create a new Lambda function, which opens the AWS Lambda console.
To use a Lambda in a different Region or account, in the Invoke AWS Lambda function, under Select a function, you can enter the ARN of a Lambda. Then set up the corresponding resource-based policy on that Lambda to allow the flow to call it.
To call lambda:AddPermission, you need to:
- Set the principal to connect.amazonaws.com
- Set the source account to be the account your instance is in.
- Set the source ARN to the ARN of your instance.

For more information, see Granting function access to other accounts.

5. Choose Add Lambda Function. Confirm that the ARN of the function is added under Lambda Functions.

Now you can refer to that Lambda function in your flows.

Invoke a Lambda function from a flow

1. Open or create a flow.
2. Add an Invoke AWS Lambda function block (in the Integrate group) to the grid. Connect the branches to and from the block.
3. Choose the title of the Invoke AWS Lambda function block to open its properties page.
4. Under Select a function, choose from the list of functions you've added to your instance.
5. (Optional) Under Function input parameters, choose Add a parameter. You can specify key-value pairs that are sent to the Lambda function when it is invoked. You can also specify a Timeout value for the function.
6. In Timeout (max 8 seconds), specify how long to wait for Lambda to time out. After this time, the contact routes down the Error branch.
For every Lambda function invocation from a flow, you pass a default set of information related to ongoing contact, as well as any additional attributes defined in the **Function input parameters** section for the **Invoke AWS Lambda function** block added.

The following is an example JSON request to a Lambda function:

```json
{
   "Details": {
      "ContactData": {
         "Attributes": {
            "exampleAttributeKey1": "exampleAttributeValue1"
         },
         "Channel": "VOICE",
         "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
         "CustomerEndpoint": {
            "Address": "+1234567890",
            "Type": "TELEPHONE_NUMBER"
         },
         "CustomerId": "someCustomerId",
         "Description": "someDescription",
         "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
         "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
         "LanguageCode": "en-US",
         "MediaStreams": {
            "Customer": {
               "Audio": {
                  "StartTimestamp": "1571360125131", // Epoch time value
                  "StopTimestamp": "1571360126131",
                  "StartFragmentNumber": "100" // Numeric value for fragment number
               }
            }
         },
         "Name": "ContactFlowEvent",
         "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
         "Queue": {
```
The request is divided into two parts:

- **Contact data**—This is always passed by Amazon Connect for every contact. Some parameters are optional.

  This section may include attributes that have been previously associated with a contact, such as when using a **Set contact attributes** block in a flow. This map may be empty if there aren't any saved attributes.

  The following image shows where these attributes would appear in the properties page of a **Set contact attributes**.
• Parameters—These are parameters specific to this call that were defined when you created the Lambda function. The following image shows where these parameters would appear in the properties page of the **Invoke AWS Lambda function** block.
The Invoke Lambda block can receive input parameters in JSON format, accommodating both primitive data types and nested JSON. The following is an example of a JSON input that can be utilized in the Invoke Lambda block.

```json
{
    "Name": "Jane",
    "Age": 10,
    "isEnrolledInSchool": true,

```
Invocation retry policy

If your Lambda invocation in a flow gets throttled, the request will be retried. It will also be retried if a general service failure (500 error) happens.

When a synchronous invocation returns an error, Amazon Connect retries up to 3 times, for a maximum of 8 seconds. At that point, the flow will progress down the Error branch.

To learn more about how Lambda retries, see Error Handling and Automatic Retries in AWS Lambda.

Invoke multiple Lambda functions

Customers hear silence while a Lambda function executes. We recommend adding a Play prompt block between functions to keep customers engaged and aware of the long interaction.

Configure your Lambda function to parse the event

To successfully pass attributes and parameters between your Lambda function and Amazon Connect, configure your function to correctly parse the JSON request sent from the Invoke AWS Lambda function block or Set contact attributes, and define any business logic that should be applied. How the JSON is parsed depends on the runtime you use for your function.

For example, the following code shows how to access exampleParameterKey1 from Invoke AWS Lambda function block and exampleAttributeKey1 from Set contact attributes block using Node.JS:

```javascript
exports.handler = function(event, context, callback) {
  // Example: access value from parameter (Invoke AWS Lambda function)
  let parameter1 = event['Details']['Parameters']['exampleParameterKey1'];

  // Example: access value from attribute (Set contact attributes block)
  let attribute1 = event['Details']['ContactData']['Attributes']['exampleAttributeKey1'];
};
```
// Example: access customer's phone number from default data
let phone = event['Details']['ContactData']['CustomerEndpoint']['Address'];

// Apply your business logic with the values
// ...

Verify the function response

The Lambda function response could be either a STRING_MAP or JSON and has to be set while configuring the **Invoke AWS Lambda function** block in the flow. If response validation is set to STRING_MAP, then the lambda function should return a flat object of key/value pairs of the string type. Otherwise, if response validation is set to JSON, the lambda function can return any valid JSON including nested JSON.
Invoke AWS Lambda function

Makes a call to AWS Lambda and optionally returns key/value pairs, which can be used to set contact attributes. Info

Function ARN

- Set manually
  
  Add a function

  ConnectLambda

- Set dynamically

Function input parameters

Add a parameter

Timeout

Timeout

3

max. 8 seconds

Response validation

Validates lambda responses to support any valid JSON or flat object of key/value pairs of string type. Info

- STRING MAP
  
  Lambda returns a flat object of key/value pairs of string type.

- JSON
The lambda response can be up to 32kb. If you fail to reach Lambda, the function throws an exception, the response is not understood, or the Lambda function takes more time than the limit, the flow jumps to the Error label.

Test the output returned from your Lambda function to confirm that it will be correctly consumed when returned to Amazon Connect. The following example shows a sample response in Node.JS:

```javascript
exports.handler = function(event, context, callback) {
    // Extract data from the event object
    let phone = event['Details']['ContactData']['CustomerEndpoint']['Address'];

    // Get information from your APIs
    let customerAccountId = getAccountIdByPhone(phone);
    let customerBalance = getBalanceByAccountId(customerAccountId);

    let resultMap = {
        AccountId: customerAccountId,
        Balance: '$' + customerBalance,
    }

    callback(null, resultMap);
}
```

This example shows an example response using Python:

```python
def lambda_handler(event, context):

    phone = event['Details']['ContactData']['CustomerEndpoint']['Address']

    customerAccountId = getAccountIdByPhone(phone)
    customerBalance = getBalanceByAccountId(customerAccountId)

    resultMap = {
        "AccountId": customerAccountId,
        "Balance": '$%s' % customerBalance
    }

    return resultMap
```

Verify the function response
The output returned from the function must be a flat object of key/value pairs, with values that include only alphanumeric, dash, and underscore characters. The size of the returned data must be less than 32 KB of UTF-8 data.

The following example shows the JSON output from these Lambda functions:

```
{
    "AccountId": "a12345689",
    "Balance": "$1000"
}
```

If response validation is set to JSON, then lambda function can return even a nested JSON, for example:

```
{
    "Name": {
        "First": "John",
        "Last": "Doe"
    },
    "AccountId": "a12345689",
    "OrderIds": ["x123", "y123"]
}
```

You may return any result as long as they are simple key-value pairs.

**Consume the Lambda function response**

There are two ways to use the function response in your flow. You can either directly reference the variables returned from Lambda, or store the values returned from the function as contact attributes and then reference the stored attributes. When you use an external reference to a response from a Lambda function, the reference will always receive the response from the most recently invoked function. To use the response from a function before a subsequent function is invoked, the response must be saved as a contact attribute, or passed as a parameter to the next function.

1. **Access variables directly**

If you access the variables directly, you can use them in flow blocks, but they are not included in contact records. To access these variables directly in a flow block, add the block after the **Invoke AWS Lambda function** block, and then reference the attributes as shown in the following example:
Name - $.External.Name
Address - $.External.Address
CallerType - $.External.CallerType

The following image shows the properties page of the **Play prompt** block. The variables are specified in the text-to-speech block.

- Select from the prompt library (audio)
- Text-to-speech or chat text
  - Enter text
    
    Your id is <say-as interpret-as="characters">$.External.AccountId</say-as>.
    
    Your balance is <say-as interpret-as="cardinal">$.External.Balance</say-as>

- Enter dynamically

  Interpret as

  SSML

Make sure that the name specified for the source attribute matches the key name returned from Lambda.

### 2. Store variables as contact attributes

If you store the variables as contact attributes, you can use them throughout your flow, and they are included in contact records.

To store the values returned as contact attributes and then reference them, use a **Set contact attributes** block in your flow after the **Invoke AWS Lambda function** block. Choose **Use attribute**, **External** for the **Type**. Following the example we're using, set **Destination Attribute** to MyAccountId, and set the **attribute** to AccountId, and do the same for MyBalance and **Balance**. This configuration is shown in the following image.
```python
import json

def lambda_handler(event, context):
    phone = event['Details']['ContactData']['CustomerEndpoint']['Address']
    customerAccountId = getAccountIdByPhone(phone)
    customerBalance = getBalanceByAccountId(customerAccountId)

    resultMap = {
        "AccountId": customerAccountId,
        "Balance": f"${%s}" % customerBalance
    }

    return resultMap
```
Add Address as a **Source attribute** and use `returnedContactAddress` as the **Destination key**. Then add CallerType as a **Source attribute** and use `returnedContactType` for the **Destination key**, as shown in the following image.

![Prompt](image)

Make sure that the name specified for the source external attribute matches the key name returned from Lambda.

**Tutorial: Create a Lambda function and invoke in a flow**

**Step 1: Create the Lambda example**

1. Sign in to the AWS Management Console and open the AWS Lambda console at [https://console.aws.amazon.com/lambda/](https://console.aws.amazon.com/lambda/).
2. In AWS Lambda, choose **Create function**.
3. Choose **Author from scratch**, if it's not selected already. Under **Basic information**, for **Function name**, enter **MyFirstConnectLambda**. For all other options, accept the defaults. These options are shown in the following image of the AWS Lambda console.
4. Choose **Create function**.

5. In the **Code source** box, in the **index.js** tab, delete the template code from the code editor.

6. Copy and paste the following code into the code editor as shown in the following image:
exports.handler = async (event, context, callback) => {

// Extract information
const customerNumber = event.Details.ContactData.CustomerEndpoint.Address;
const companyName = event.Details.Parameters.companyName;

// Fetch data
const balance = await fetchBalance(customerNumber, companyName);
const support = await fetchSupportUrl(companyName);

// Prepare result
const resultMap = {
  customerBalance: balance,
  websiteUrl: support
};
callback(null, resultMap);
}

async function fetchBalance(customerPhoneNumber, companyName) {

// Get data from your API Gateway or Database like DynamoDB
return Math.floor(Math.random() * 1000);
}

async function fetchSupportUrl(companyName) {

// Get data from your API Gateway or Database like DynamoDB
return 'www.GGG.com/support';
}
This code is going to generate a random result for the customerBalance.

7. Choose **Deploy**.

8. After you choose **Deploy**, choose **Test** to launch the test editor.

9. In the **Configure test event** dialog box, select **Create new event**. For **Event name**, enter **ConnectMock** as the test name.

10. In the **Event JSON** box, delete the sample code and enter the following code instead.

```json
{
  "Details": {
    "ContactData": {
      "Attributes": {},
      "Channel": "VOICE",
      "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
      "CustomerEndpoint": {
        "Address": "+1234567890",
        "Type": "TELEPHONE_NUMBER"
      },
      "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
      "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
      "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/c8c0e68d-2200-4265-82c0-XXXXXXXXX",
      "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
      "Queue": {
        "Name": "PasswordReset"
      },
      "SystemEndpoint": {
        "Address": "+1234567890",
        "Type": "TELEPHONE_NUMBER"
      }
    },
    "Parameters": {
      "companyName": "GGG"
    }
  },
  "Name": "ContactFlowEvent"
}
```
11. Choose **Save**.

12. Choose **Test**. You should see the following something similar to the following image:

   ![Code source window with Test button highlighted](image)

   Your balance will be different. The code generates a random number.

**Step 2: Add your Lambda to Amazon Connect**


2. Choose your Amazon Connect instance alias.

   ![Amazon Connect virtual contact center instances](image)

3. On the navigation menu, choose **Flows**.

4. In the AWS Lambda section, use the **Lambda Functions** dropdown box to select **MyFirstConnectLambda**.
5. Choose **Add Lambda Function**.

### Step 3: Create the contact flow

The following image is an example of the flow you are going to build using the steps in this procedure. It contains the following blocks: **Set contact attributes**, **Play prompt**, **Invoke AWS Lambda function**, another **Set contact attributes** block, another **Play prompt** block, and finally a **Disconnect** block.

1. Log in to the Amazon Connect admin website at [https://instance name.my.connect.aws/](https://instance name.my.connect.aws/).
2. On the navigation menu, go to Routing, Flows, Create a contact flow.

3. Drag a Set contact attributes block onto the grid, and configure its properties page shown in the following image:

   - **Namespace** = User defined.
   - **Attribute** = companyName.
   - Choose **Set manually**. **Value** = GGG.
   - Choose **Save**.

4. Drag a Play prompt block onto the grid, and configure its properties page as shown in the following image:
a. Choose **Text-to-speech or chat text**, **Set manually**, and set **Interpret as** to **SSML**. Enter the following text in the box for the text to be spoken:

    Hello, thank you for calling $.Attributes.companyName inc.

b. Choose **Save**.

5. Drag another **Play prompt** block onto the grid, and configure its properties page as shown in the following image:
a. Choose **Text-to-speech or chat text**, **Set manually**, and set **Interpret as** to **Text**. Enter the following text in the box for the text to be spoken:

   **Please try again later.**

b. Choose **Save**.

6. Drag a [Invoke AWS Lambda function](#) block onto the grid, and configure its properties page as shown in the following image:
Choose **Select manually**, and then choose **MyFirstConnectLambda** from the dropdown.

In the **Destination Key** box, enter **companyName**. (This is sent to Lambda.)

Choose **Set dynamically** box

For **Namespace**, select **User Defined**.

For **Attribute**, enter **companyName**.

Choose **Save**.

7. Drag a **Set contact attributes** block onto the grid, choose **Add another attribute**, and configure its properties page as shown in the following image:
a. **Namespace** = User Defined. **Attribute** = MyBalance.

b. Choose **Set dynamically**.

c. **Namespace** = External.

d. **Attribute** = customerBalance. This is the result from Lambda.

e. Choose **Add another attribute**.

f. **Namespace** = User-defined.

g. **Attribute** = MyURL.

h. Select **Set dynamically.** **Namespace** = External.
i. **Attribute** = `websiteUrl`. This is the result from Lambda.

j. Choose **Save**.

8. Drag a **Play prompt** block onto the grid, and configure its properties page as shown in the following image:

![Play prompt block configuration](image)

a. Choose **Text-to-speech or chat text**, and set **Interpret as** to **SSML**. Enter the following text in the box:

   Your remaining balance is `<say-as interpret-as="characters">$.Attributes.MyBalance</say-as>`.

   Thank you for calling `$Attributes.companyName`.

   Visit `$Attributes.MyURL` for more information.

b. Choose **Save**.

9. Drag a **Disconnect / hang up** block onto the grid.

10. Connect the all blocks so your flow looks like the image shown at the top of this procedure.

11. Enter **MyFirstConnectFlow** as the name, and then choose **Publish**.

12. On the navigation menu, go to **Channels, Phone numbers**.
13. Select your phone number.

Now try it out. Call the number. You should hear a greeting message, your balance, and the website to visit.

**Set up live media streaming of customer audio**

In Amazon Connect, you can capture customer audio during an interaction with your contact center by sending the audio to a Kinesis video stream. Depending on your settings, audio can be captured for the entire interaction—until the interaction with the agent is complete—or only one direction:

- What the customer hears, including what the agent says and system prompts.
- What the customer says, including when they are on hold.

The customer audio streams also include interactions with an Amazon Lex bot, if you're using one in your flow.

You can perform analysis on the audio streams to determine customer sentiment, use the audio for training purposes, or to later review the audio to identify and flag abusive callers.

**Contents**

- Plan for live media streaming
- Enable live media streaming in your instance
- How to access Kinesis Video Streams data
- Example flow for testing live media streaming
- Contact attributes for live media streaming

**Plan for live media streaming**

⚠️ **Important**

If you want to use the audio streaming feature, you need to retain the streams that are created by Amazon Connect. Don't delete them, unless you're going to stop using the streaming feature.
You can send all audio to and from the customer to Kinesis Video Streams. Media streaming leverages Kinesis Video Streams multi-track support so that what the customer says is on a separate track from what the customer hears.

Audio sent to Kinesis uses a sampling rate of 8 kHz.

**Do you need to increase your service quotas?**

When you enable media streaming in Amazon Connect, one Kinesis video stream is used per active call. By default we allocate 50 streams per instance to your account. We automatically create additional streams as needed to keep pace with active calls, unless your account reaches the **Kinesis Video Streams service quota**.

Contact AWS Support to request an increase to **Number of Streams**.

To request an increase to your service quota, in the AWS Support Center, choose **Create Case** and then choose **Service Quota Increase**.

---

**Tip**

We make sure that **PutMedia** requests always stay within the 5 TPS quota. You don't need to request an increase.

---

**How long do you need to store audio?**

Customer audio is stored in Kinesis for the time defined by your retention settings in an Amazon Connect instance. For instructions for setting this value, see **Enable live media streaming in your instance**.

**Do you need to change the audio streams?**

We recommend that you refrain from modifying the streams. Doing so can cause unexpected behavior.

**Who requires IAM permissions to retrieve data?**

If your business is using IAM permissions, your AWS admin will need to grant permissions to people who are going to retrieve data from Kinesis Video Streams. They'll need to grant them full access permissions for Kinesis Video Streams and AWS Key Management Service.
Enable live media streaming in your instance

Live media streaming (customer audio streams) is not enabled by default. You can enable customer audio streams from the settings page for your instance.

To enable live media streaming

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. In the navigation pane, choose Data storage.
5. Enter a prefix for the Kinesis Video Streams created for your customer audio. This prefix makes it easier for you to identify the stream with the data.
6. Choose the KMS key to use to encrypt the data sent to Kinesis. The KMS key must be in the same Region as the instance.
7. Specify a number and unit for the Data retention period.

⚠️ Important
If you select No data retention, data is not retained and is available to be consumed for only 5 minutes. This is the default minimum time that Kinesis retains data. Because Amazon Connect uses Kinesis for streaming, Kinesis quotas apply.

8. Choose Save under Live media streaming, and then choose Save at the bottom of the page.

After you enable live media streaming, add Start media streaming and Stop media streaming blocks to your flow. Configure those blocks to specify what audio you want to capture. For instructions and an example, see Example flow for testing live media streaming.

How to access Kinesis Video Streams data

You must have developer skills to work with Kinesis Video Streams data. Use the code samples in this section to interact with the customer audio data sent to Kinesis Video Streams.

Contents
LMSDemo.java

```java
package com.amazonaws.kinesisvideo.parser.demo;

import com.amazonaws.auth.AWSSessionCredentials;
import com.amazonaws.auth.AWSSessionCredentialsProvider;
import com.amazonaws.kinesisvideo.parser.examples.LMSExample;
import com.amazonaws.regions.Regions;

import java.io.FileOutputStream;
import java.io.IOException;

public class LMSDemo {

    public static void main(String args[]) throws InterruptedException, IOException {
        LMSExample example = new LMSExample(Regions.US_WEST_2,
                "<<StreamName>>",
                "<<FragmentNumber>>",
                new AWSSessionCredentialsProvider() {
                    @Override
                    public AWSSessionCredentials getCredentials() {
                        return new AWSSessionCredentials() {
                            @Override
                            public String getSessionToken() {
                                return "<<AWSSessionToken>>";
                            }
                            @Override
                            public String getAWSAccessKeyId() {
                                return "<<AWSAccessKey>>";
                            }
                            @Override
                            public String getAWSSecretKey() {
                                return "<<AWSSecretKey>>";
                            }
                        };
                    }
                    @Override
                    public void refresh() {}
                }
                "<<StreamName>>",
                "<<FragmentNumber>>",
                new AWSSessionCredentialsProvider() {
                    @Override
                    public AWSSessionCredentials getCredentials() {
                        return new AWSSessionCredentials() {
                            @Override
                            public String getSessionToken() {
                                return "<<AWSSessionToken>>";
                            }
                            @Override
                            public String getAWSAccessKeyId() {
                                return "<<AWSAccessKey>>";
                            }
                            @Override
                            public String getAWSSecretKey() {
                                return "<<AWSSecretKey>>";
                            }
                        };
                    }
                    @Override
                    public void refresh() {}
                };
```
package com.amazonaws.kinesisvideo.parser.examples;

import com.amazonaws.auth.AWSCredentialsProvider;
import com.amazonaws.kinesisvideo.parser.ebml.MkvTypeInfos;
import com.amazonaws.kinesisvideo.parser.mkv.MkvDataElement;
import com.amazonaws.kinesisvideo.parser.mkv.MkvElementVisitException;
import com.amazonaws.kinesisvideo.parser.mkv.MkvElementVisitor;
import com.amazonaws.kinesisvideo.parser.mkv.MkvEndMasterElement;
import com.amazonaws.kinesisvideo.parser.mkv.MkvStartMasterElement;
import com.amazonaws.kinesisvideo.parser.utilities.FragmentMetadataVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.FrameVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.LMSFrameProcessor;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.kinesisvideo.model.StartSelector;
import com.amazonaws.services.kinesisvideo.model.StartSelectorType;
import java.io.Closeable;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.OutputStream;
import java.io.PipedInputStream;
import java.io.PipedOutputStream;
import java.util.concurrent.ExecutorService;
import java.util.concurrent.Executors;
import java.util.concurrent.TimeUnit;

LMSExample.java
public class LMSExample extends KinesisVideoCommon {

    private final ExecutorService executorService;
    private GetMediaProcessingArguments getMediaProcessingArguments;
    private final StreamOps streamOps;
    private final OutputStream outputStreamFromCustomer;
    private final OutputStream outputStreamToCustomer;
    private final String fragmentNumber;

    public LMSExample(Regions region,
                        String streamName,
                        String fragmentNumber,
                        AWSCredentialsProvider credentialsProvider,
                        OutputStream outputStreamFromCustomer,
                        OutputStream outputStreamToCustomer) throws IOException {
        super(region, credentialsProvider, streamName);
        this.streamOps = new StreamOps(region, streamName, credentialsProvider);
        this.executorService = Executors.newFixedThreadPool(2);
        this.outputStreamFromCustomer = outputStreamFromCustomer;
        this.outputStreamToCustomer = outputStreamToCustomer;
        this.fragmentNumber = fragmentNumber;
    }

    public void execute () throws InterruptedException, IOException {
        getMediaProcessingArguments = GetMediaProcessingArguments.create(outputStreamFromCustomer, outputStreamToCustomer);
        try (GetMediaProcessingArguments getMediaProcessingArgumentsLocal = getMediaProcessingArguments) {
            //Start a GetMedia worker to read and process data from the Kinesis Video Stream.
            GetMediaWorker getMediaWorker = GetMediaWorker.create(getRegion(),
                                                                    getCredentialsProvider(),
                                                                    getStreamName(),
                                                                    new StartSelector().withStartSelectorType(StartSelectorType.FRAGMENT_NUMBER).withAfterFragmentNumber(fragmentNumber),
                                                                    streamOps.amazonKinesisVideo, 
                                                                    getMediaProcessingArgumentsLocal.getFrameVisitor());
            executorService.submit(getMediaWorker);

            //Wait for the workers to finish.
            executorService.shutdown();
            executorService.awaitTermination(120, TimeUnit.SECONDS);
            if (!executorService.isTerminated()) {


System.out.println("Shutting down executor service by force");
executorService.shutdownNow();
} else {
    System.out.println("Executor service is shutdown");
}
} finally {
    outputStream.close();
}

private static class LogVisitor extends MkvElementVisitor {
    private final FragmentMetadataVisitor fragmentMetadataVisitor;
    private LogVisitor(FragmentMetadataVisitor fragmentMetadataVisitor) {
        this.fragmentMetadataVisitor = fragmentMetadataVisitor;
    }
    public long getFragmentCount() {
        return fragmentCount;
    }
    private long fragmentCount = 0;
    @Override
    public void visit(MkvStartMasterElement startMasterElement) throws MkvElementVisitException {
        if (MkvTypeInfos.EBML.equals(startMasterElement.getElementMetaData().getTypeInfo())) {
            fragmentCount++;
            System.out.println("Start of segment");
        }
    }
    @Override
    public void visit(MkvEndMasterElement endMasterElement) throws MkvElementVisitException {
        if (MkvTypeInfos.SEGMENT.equals(endMasterElement.getElementMetaData().getTypeInfo())) {
            System.out.println("End of segment");
        }
    }
private static class GetMediaProcessingArguments implements Closeable {

    public FrameVisitor getFrameVisitor() {
        return frameVisitor;
    }

    private final FrameVisitor frameVisitor;

    public GetMediaProcessingArguments(FrameVisitor frameVisitor) {
        this.frameVisitor = frameVisitor;
    }

    public static GetMediaProcessingArguments create(OutputStream outputStreamFromCustomer, OutputStream outputStreamToCustomer) throws IOException {
        // Fragment metadata visitor to extract Kinesis Video fragment metadata from the GetMedia stream.
        FragmentMetadataVisitor fragmentMetadataVisitor = FragmentMetadataVisitor.create();

        // A visitor used to log as the GetMedia stream is processed.
        LogVisitor logVisitor = new LogVisitor(fragmentMetadataVisitor);

        // A composite visitor to encapsulate the three visitors.
        FrameVisitor frameVisitor = FrameVisitor.create(LMSFrameProcessor.create(outputStreamFromCustomer, outputStreamToCustomer, fragmentMetadataVisitor));

        return new GetMediaProcessingArguments(frameVisitor);
    }

    @Override
    public void close() throws IOException {
    }
}
public class LMSFrameProcessor implements FrameVisitor.FrameProcessor {

    private OutputStream outputStreamFromCustomer;
    private OutputStream outputStreamToCustomer;
    private FragmentMetadataVisitor fragmentMetadataVisitor;

    protected LMSFrameProcessor(OutputStream outputStreamFromCustomer, OutputStream outputStreamToCustomer, FragmentMetadataVisitor fragmentMetadataVisitor) {
        this.outputStreamFromCustomer = outputStreamFromCustomer;
        this.outputStreamToCustomer = outputStreamToCustomer;
    }

    public static LMSFrameProcessor create(OutputStream outputStreamFromCustomer, OutputStream outputStreamToCustomer, FragmentMetadataVisitor fragmentMetadataVisitor) {
        return new LMSFrameProcessor(outputStreamFromCustomer, outputStreamToCustomer, fragmentMetadataVisitor);
    }

    @Override
    public void process(Frame frame, MkvTrackMetadata trackMetadata) {
        saveToOutputStream(frame);
    }

    private void saveToOutputStream(final Frame frame) {
        ByteBuffer frameBuffer = frame.getFrameData();
        long trackNumber = frame.getTrackNumber();
        MkvTrackMetadata metadata = fragmentMetadataVisitor.getMkvTrackMetadata(trackNumber);
        String trackName = metadata.getTrackName();
try {
    byte[] frameBytes = new byte[frameBuffer.remaining()];
    frameBuffer.get(frameBytes);
    if (Strings.isNullOrEmpty(trackName) ||
    "AUDIO_FROM_CUSTOMER".equals(trackName)) {
        outputStreamFromCustomer.write(frameBytes);
    } else if ("AUDIO_TO_CUSTOMER".equals(trackName)) {
        outputStreamToCustomer.write(frameBytes);
    } else {
        // Unknown track name. Not writing to output stream.
    }
}

} catch (IOException e) {
    e.printStackTrace();
}

Example flow for testing live media streaming

Here's how you can set up a flow to test live media streaming:

1. Add a **Start media streaming** block at the point where you want to enable customer audio streaming.
2. Connect the **Success** branch to the rest of your flow.
3. Add a **Stop media streaming** block to where you want to stop streaming.
4. Configure both blocks to specify what you want to stream: **From the customer** and/or **To the customer**.
Customer audio is captured until a **Stop media streaming** block is invoked, even if the contact is passed to another flow.

Use the contact attributes for media streaming in your flow so that the contact record includes the attributes. You can then view the contact record to determine the media streaming data associated with a specific contact. You can also pass the attributes to an AWS Lambda function.

The following example flow shows how you might use media streaming with attributes for testing purposes. This flow includes a **Start media streaming** block but it is missing the **Stop media streaming** block.
After the audio is successfully streamed to Kinesis Video Streams, the contact attributes are populated from the **Invoke AWS Lambda function** block. You can use the attributes to identify the location in the stream where the customer audio starts. For instructions, see [Contact attributes for live media streaming](#).

### Contact attributes for live media streaming

The attributes are displayed when you select **Media streams** for the **Type** in a flow block that supports attributes, such as the **Start media streaming** block. They include the following:

**Customer audio stream ARN**

The ARN of the Kinesis video stream that includes the customer data to reference.


**Customer audio start timestamp**

The time at which the customer audio stream started.

Customer audio stop timestamp

The time at which the customer audio stream stopped.

**JSONPath format:** `$.MediaStreams.Customer.Audio.StopTimestamp`

Customer audio start fragment number

The number that identifies the Kinesis Video Streams fragment in which the customer audio stream started.

**JSONPath format:** `$.MediaStreams.Customer.Audio.StartFragmentNumber`

For more information about Amazon Kinesis Video Streams fragments, see [Fragment](#) in the Amazon Kinesis Video Streams Developer Guide.

### Encrypt customer input

You can encrypt sensitive data that is collected by flows. To do this, you need to use public-key cryptography.

When configuring Amazon Connect, you first provide the public key. This is the key used when encrypting data. Later, you provide the X.509 certificate, which includes a signature that proves you possess the private key.

In a flow that collects data, you provide an X.509 certificate to encrypt data that's captured using the **Stored customer input** system attribute. You must upload the key in `.pem` format to use this feature. The encryption key is used to verify the signature of the certificate used within the flow.

**Note**

You can have up to two encryption keys active at one time to facilitate rotation.

To decrypt the data in the **Stored customer input** attribute, use the AWS Encryption SDK. For more information, see the AWS Encryption SDK Developer Guide.

For a detailed walkthrough, see Creating a secure IVR solution with Amazon Connect. It shows how to:

- Configure Amazon Connect to collect a credit card number.
- Encrypt the credit card digits.
- Send it to our backend AWS Lambda for decryption, using the customer supplied decryption key.

It provides two commands using OpenSSL:

- One to generate an RSA key pair and a self-signed X.509 certificate
- Another to extract the public key from the RSA key pair

**How to decrypt data encrypted by Amazon Connect**

The following code sample shows how to decrypt data using the AWS Encryption SDK.

```java
package com.amazonaws;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import java.io.IOException;
import java.nio.charset.Charset;
import java.nio.file.Files;
import java.nio.file.Paths;
import java.security.GeneralSecurityException;
import java.security.KeyFactory;
import java.security.Security;
import java.security.interfaces.RSAPrivateKey;
import java.security.spec.PKCS8EncodedKeySpec;
import java.util.Base64;

public class AmazonConnectDecryptionSample {

    // The Provider 'AmazonConnect' is used during encryption, this must be used during decryption for key to be found
    private static final String PROVIDER = "AmazonConnect";

    // The wrapping algorithm used during encryption
    private static final String WRAPPING_ALGORITHM = "RSA/ECB/OAEPWithSHA-512AndMGF1Padding";
```
/**
 * This sample show how to decrypt data encrypted by Amazon Connect.
 * To use, provide the following command line arguments: [path-to-private-key]
 * [key-id] [cyphertext]
 * Where:
 * path-to-private-key is a file containing the PEM encoded private key to use for decryption
 * key-id is the key-id specified during encryption in your flow
 * cyphertext is the result of the encryption operation from Amazon Connect
 */

public static void main(String[] args) throws IOException, GeneralSecurityException {
    String privateKeyFile = args[0]; // path to PEM encoded private key to use for decryption
    String keyId = args[1]; // this is the id used for key in your flow
    String cypherText = args[2]; // the result from flow

    Security.addProvider(new BouncyCastleProvider());

    // read the private key from file
    String privateKeyPem = new String(Files.readAllBytes(Paths.get(privateKeyFile)), Charset.forName("UTF-8"));
    RSAPrivateKey privateKey = getPrivateKey(privateKeyPem);

    AwsCrypto awsCrypto = new AwsCrypto();
    JceMasterKey decMasterKey =
        JceMasterKey.getInstance(null, privateKey, PROVIDER, keyId, WRAPPING_ALGORITHM);
    CryptoResult<String, JceMasterKey> result =
        awsCrypto.decryptString(decMasterKey, cypherText);

    System.out.println("Decrypted: " + result.getResult());
}

public static RSAPrivateKey getPrivateKey(String privateKeyPem) throws IOException,
    GeneralSecurityException {
    String privateKeyBase64 = privateKeyPem
        .replace("-----BEGIN RSA PRIVATE KEY-----\n", "")
        .replace("-----END RSA PRIVATE KEY-----", "")
        .replaceAll("\n", "");

    byte[] decoded = Base64.getDecoder().decode(privateKeyBase64);
    KeyFactory kf = KeyFactory.getInstance("RSA");
    PKCS8EncodedKeySpec keySpec = new PKCS8EncodedKeySpec(decoded);
Track events as customers interact with flows

Amazon Connect flow logs provide you with real-time details about events in your flows as customers interact with them. You can also use flow logs to help debug your flows as you are creating them. If needed, you can always roll back to a previous version of a flow.

Contents

- Flow logs stored in an Amazon CloudWatch log group
- Enable flow logs
- Search flow logs
- What data is gathered in flow logs
- Track customers between flows
- Create alerts for flow log events

Flow logs stored in an Amazon CloudWatch log group

Flow logs are stored in an Amazon CloudWatch log group, in the same AWS Region as your Amazon Connect instance. This log group is created automatically when Enable flow logging is turned on for your instance.

For example, the following image shows the CloudWatch log groups for two test instances.
A log entry added as each block in your flow is triggered. You can configure CloudWatch to send alerts when unexpected events occur during active flows.

**What happens if my log group is deleted?** You need to manually re-create the CloudWatch log group. Otherwise, Amazon Connect won't publish more logs.

**Pricing for flow logging**

You are not charged for generating flow logs, but you are charged for using CloudWatch for generating and storing the logs. Free tier customers are charged only for usage that exceeds service quotas. For details about Amazon CloudWatch pricing, see [Amazon CloudWatch Pricing](#).

**Enable flow logs**

**Tip**

Amazon Connect delivers flow logs at least once. They may be delivered again for multiple reasons. For example, a service retry due to an unavoidable failure.
Step 1: Enable logging for your instance

By default when you create a new Amazon Connect instance, an Amazon CloudWatch log group is created automatically to store the logs for your instance.

Use the following procedure to check that logging is enabled for your instance.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. In the navigation pane, choose Flows.
4. Select Enable Flow logs and choose Save.

Step 2: Add the Set logging behavior block

Logs are generated only for flows that include a Set logging behavior block with logging set to enabled.

You control which flows, or parts of flows, logs are generated for by including multiple Set logging behavior blocks and configuring them as needed.

When you use a Set logging behavior block to enable or disable logging for a flow, logging is also enabled or disabled for any subsequent flow that a contact is transferred to, even if the flow does not include a Set logging behavior block. To avoid logging that persists between flows, enable or disable a Set logging behavior block as needed for that specific flow.
To enable or disable flow logs for a flow

1. In the flow designer, add a Set logging behavior block and connect it to another block in the flow.
2. Open the properties for the block. Choose Enable or Disable.
3. Choose Save.
4. If you add a Set logging behavior block to a flow that is already published, you must publish it again to start generating logs for it.

Search flow logs

Before you can search flow logs, you must first enable flow logging.

Logs will be created for conversations that occur after logging is enabled.

To search flow logs

1. Open Amazon CloudWatch console, go to Logs, Log groups. The following image shows a sample log group named mytest88.
2. Choose the log group for your instance.

   A list of log streams will be displayed.

3. To search all the log streams in the instance, choose **Search log group**, as shown in the following image.

4. In the search box, enter the string you want to search for, for example, all or a portion of the contact ID.

5. After a couple of moments (longer depending on how big your log is), Amazon CloudWatch returns results. The following image shows a sample contact ID **fb3304c2**, and the result.
6. You can open each event to see what happened. The following image shows the event for when a **Play prompt** block runs in a flow.

---

**What data is gathered in flow logs**

Log entries for flows include details about the block associated with the log entry, the contact ID, and the action taken after the steps in the block were completed. Any contact interaction that occurs outside of the flow is not logged, such as time spent in a queue or interactions with an agent.

You can set the properties of the block to disable logging during the parts of your flow that interact with or capture sensitive data or customers' personal information.
If you use Amazon Lex or AWS Lambda in your flows, the logs show the entry and exit of the flow going to them, and include any information about the interaction that is sent or received during entry or exit.

Because the logs also include the flow ID, and the flow ID stays the same when you change a flow, you can use the logs to compare the interactions with different versions of the flow.

The following example log entry shows a **Set working queue** block of an inbound flow.

```json
{
  "ContactId": "11111111-2222-3333-4444-555555555555",
  "ContactFlowModuleType": "SetQueue",
  "Timestamp": "2021-04-13T00:14:31.581Z",
  "Parameters": {
  }
}
```

### Track customers between flows

In many cases, customers interact with multiple flows in your contact center, being passed from one flow to another to appropriately assist them with their specific issue. Flow logs help you track customers between different flows, by including the ID of the contact in each log entry.

When a customer is transferred to a different flow, the ID for the contact associated with their interaction is included with the log for the new flow. You can query the logs for the contact ID to trace the customer interaction through each flow.

In larger, high-volume contact centers, there can be multiple streams for flow logs. If a contact is transferred to a different flow, the log may be in a different stream. To make sure that you are finding all of the log data for a specific contact, you should search for the contact ID in the entire CloudWatch log group instead of in a specific log stream.

### Create alerts for flow log events

You can configure CloudWatch to define a filter pattern that looks for specific events in your flow logs and then creates an alert when an entry for that event is added to the log.
For example, you can set an alert for when a flow block goes down an error path as a customer interacts with the flow. Log entries are typically available in CloudWatch within a short time, giving you near real-time notification of events in flows.

**Use Amazon Connect contact attributes**

One way to make your customers feel cared for is to create personalized experiences for them in your contact center. For example, you can deliver one welcome message for customers who are using a phone and another for customers using chat. To do this, you need a way to store information about the contact and then make a decision based on the value.

**Contents**

- What is a contact attribute?
- List of available contact attributes and their JSONPath reference
- How to reference contact attributes
- Display contact information to the agent in the CCP
- Route based on number of contacts in a queue
- Route based on contact's channel
- Use Amazon Lex and attributes
- Lambda functions and attributes

**What is a contact attribute?**

In Amazon Connect, each interaction with a customer is a contact. The interaction can be a phone call (voice), a chat, or an automated interaction using an Amazon Lex bot.

Each contact can have some data that is specific to a particular interaction. This data can be accessed as a contact attribute. For example:

- The name of the customer
- The name of the agent
- The channel used for the contact, such as phone or chat
- And more
A contact attribute represents this data as a key-value pair. You might think of it as a field name together with the data entered into that field.

For example, here are a couple of key-value pairs for the customer name:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>firstname</td>
<td>Jane</td>
</tr>
<tr>
<td>lastname</td>
<td>Doe</td>
</tr>
</tbody>
</table>

The advantage of contact attributes is that they enable you to store temporary information about the contact so you can use it in the flow.

For example, in your welcome messages, you can say their name or thank them for being a member. To do this, you need a way of retrieving data about that specific customer and using it in a flow.

**Common use cases**

Here are some common use cases for where contact attributes are used:

- Use the customer phone number to schedule a queued callback.
- Identify which agent is interacting with a customer so that a post call survey can be associated with a contact.
- Identify the number of contacts in a queue to decide if the contact should be routed to a different queue.
- Get the corresponding media streaming ARN to store in a database.
- Use the customer phone number to identify the status of a customer (for example, are they a member), or the status of their order (shipped, delayed, etc.) to route them to the appropriate queue.
- Based on a customer interaction with a bot, identify the slot (for example, the type of flowers to order) to be used in a flow.
Types of contact attributes

To make it faster for you to find and choose the attributes you want to use, attributes are grouped into types. For each flow block, we only surface those types of attributes that work with it.

Another way to think about types of contact attributes is to categorize them based on where the value comes from. The values for contact attributes have the following sources:

- Amazon Connect provides the value, such as the agent's name, during the contact interaction. This is known as providing the value at runtime.
- An external process, such as Amazon Lex or AWS Lambda, provides the value.
- User-defined. In the flow, you can specify the value for an attribute.

Flow attributes are similar to user-defined attributes. However, unlike user-defined attributes, flow attributes are restricted to the flow in which they are configured.

The following illustration lists the types of available contact attributes, and maps them to the three sources for the values: Amazon Connect, external process such as Amazon Lex, and user-defined.

Contact attributes in the contact record

In contact records, contact attributes are shared across all contacts with the same InitialContactId.
For example, while carrying out transfers, a contact attribute updated in the transfer flow updates the attribute's value in the contact attributes of both contact records (that is, the Inbound and Transfer contact attributes).

"$" is a special character

Amazon Connect treats the "$" character as a special character. You can't use it in a key when setting an attribute.

For example, let's say you're creating an interact block with text-to-speech. You set an attribute like this:

`{"$one":"please read this text"}`

When Amazon Connect reads this text, it reads "dollar sign one" to the contact instead of "please read this text." Also, if you were to include $ in a key and try to reference the value later using Amazon Connect, it wouldn't retrieve the value.

Amazon Connect does log and pass the full key:value pair (`{"_$one":"please read this text"}`) to integrations such as Lambda.

What happens if an attribute doesn't exist

Be sure to implement logic to handle if the attribute doesn't exist and the contact is routed down the error branch.

Let's say you add an attribute to the Store customer input block. The **Namespace** is **Agent** and the **Key** is **User name**, as shown in the following example.
If the flow runs and the agent user name is not available, then the contact is routed down the error branch.

**List of available contact attributes and their JSONPath reference**

The following tables describe the contact attributes available in Amazon Connect.

The JSONPath reference for each attribute is provided so you can [create dynamic text strings](#).

**System attributes**

These are predefined attributes in Amazon Connect. You can reference system attributes, but you cannot create them.

Not all blocks in a flow support using System attributes. For example, you cannot use a System attribute to store customer input. Instead, use a [user-defined attribute](#) to store the data input by a customer.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Region</td>
<td>When used, this returns the AWS Region where the contact is being handled. For example, us-west-2, us-east-1, and so on.</td>
<td>System</td>
<td>$.AwsRegion or $['AwsRegion']</td>
</tr>
<tr>
<td>Customer number</td>
<td>The customer's phone number.</td>
<td>System</td>
<td>$.CustomerEndpoint.Address</td>
</tr>
<tr>
<td>Customer ID</td>
<td>The customer's identification number.</td>
<td>System</td>
<td>$.CustomerId</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Dialed number</td>
<td>The number the customer dialed to call your contact center.</td>
<td>System</td>
<td>$.SystemEndpoint.Address</td>
</tr>
<tr>
<td></td>
<td>This attribute is included in contact records. When used in a Lambda function, it's included in the input object under SystemEndpoint.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Customer callback number</td>
<td>The number that Amazon Connect uses to call back the customer. This number can be the one used for a queued callback, or when an agent is dialing from the CCP. Transfer to callback queue functionality, or for an agent dialing from the CCP. The default value is the number that the customer used to call your contact center. However, it can be overwritten with the <code>Set callback number</code> block. This attribute is not included in contact records, and it's not accessible in Lambda input. However, you can copy the attribute to a user-defined attribute with the Set contact attribute block, which is included in contact records.</td>
<td>System</td>
<td>not applicable</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>records. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block, which is not included in contact records.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Stored customer input</td>
<td>An attribute created from the most recent invocation of a <strong>Store customer input</strong> block. The attribute values created from the most recent Store customer input block invocation. This attribute is not included in contact records, and is not accessible in Lambda input. You can copy the attribute to a user-defined attribute with the Set contact attribute block, which is included in contact records. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block,</td>
<td>System</td>
<td>not applicable</td>
</tr>
<tr>
<td>Queue name</td>
<td>The name of the queue.</td>
<td>System</td>
<td>$.Queue.Name</td>
</tr>
<tr>
<td>Queue ARN</td>
<td>The ARN for the queue.</td>
<td>System</td>
<td>$.Queue.ARN</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Queue outbound number</td>
<td>The Outbound caller ID number for the selected queue. This attribute is only available in outbound whisper flows.</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Text to speech voice</td>
<td>The name of the Amazon Polly voice to use for text-to-speech in a contact flow.</td>
<td>System</td>
<td>$.TextToSpeechVoiceId</td>
</tr>
<tr>
<td>Contact id</td>
<td>The unique identifier of the contact.</td>
<td>System</td>
<td>$.ContactId</td>
</tr>
<tr>
<td>Initial Contact id</td>
<td>The unique identifier for the contact associated with the first interaction between the customer and your contact center. Use the initial contact ID to track contacts between flows.</td>
<td>System</td>
<td>$.InitialContactId</td>
</tr>
<tr>
<td>Task Contact id</td>
<td>The unique identifier for the task contact. Use the task contact ID to track tasks between flows.</td>
<td>System</td>
<td>$.Task.ContactId</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Previous Contact id</td>
<td>The unique identifier for the contact before it was transferred. Use the previous contact ID to trace contacts between flows.</td>
<td>System</td>
<td>$.PreviousContactId</td>
</tr>
<tr>
<td>Channel</td>
<td>The method used to contact your contact center: VOICE, CHAT, TASK.</td>
<td>System</td>
<td>$.Channel</td>
</tr>
<tr>
<td>Instance ARN</td>
<td>The ARN for your Amazon Connect instance.</td>
<td>System</td>
<td>$.InstanceARN</td>
</tr>
<tr>
<td>Initiation method</td>
<td>How the contact was initiated. Valid values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, QUEUE_TRANSFER, DISCONNECT, and API. Initiation method doesn't work in Agent whisper flows or Customer whisper flows.</td>
<td>System</td>
<td>$.InitiationMethod</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the task.</td>
<td>System</td>
<td>$.Name</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the task.</td>
<td>System</td>
<td>$.Description</td>
</tr>
<tr>
<td>References</td>
<td>Links to other documents that are related to a contact.</td>
<td>System</td>
<td>$.References.<strong>Reference Key</strong> .Value and $.References.<strong>Reference Key</strong> .Type where <strong>ReferenceKey</strong> is the user-defined Reference name.</td>
</tr>
<tr>
<td>Language</td>
<td>The language of content.</td>
<td>System</td>
<td>$.LanguageCode</td>
</tr>
<tr>
<td></td>
<td>Use the standard java.util.Locale. For example, en-US for United States English, jp-JP for Japanese, etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Endpoint Type</td>
<td>The type of the system endpoint. Valid value is TELEPHONE _NUMBER.</td>
<td>System</td>
<td>$.SystemEndpoint.Type</td>
</tr>
<tr>
<td>Customer Endpoint type</td>
<td>The type of the customer endpoint. Valid value is TELEPHONE _NUMBER.</td>
<td>System</td>
<td>$.CustomerEndpoint.Type</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Queue Outbound Caller ID number</td>
<td>The outbound caller ID number defined for the queue. This can be useful for reverting the caller ID after setting a custom caller ID.</td>
<td>System</td>
<td>$.Queue.OutboundCallerId.Address</td>
</tr>
<tr>
<td>Queue Outbound Caller ID number type</td>
<td>The type of the outbound caller ID number. Valid value is TELEPHONE _NUMBER.</td>
<td>System</td>
<td>$.Queue.OutboundCallerId.Type</td>
</tr>
</tbody>
</table>

**Agent attributes**

The following table lists the agent attributes available in Amazon Connect.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent User name</td>
<td>The user name an agent uses to log in to Amazon Connect.</td>
<td>System</td>
<td>$.Agent.UserName</td>
</tr>
<tr>
<td>Agent First name</td>
<td>The agent's first name as entered in their Amazon Connect user account.</td>
<td>System</td>
<td>$.Agent.FirstName</td>
</tr>
<tr>
<td>Agent Last name</td>
<td>The agent's last name as entered in their Amazon Connect user account.</td>
<td>System</td>
<td>$.Agent.LastName</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Agent ARN</td>
<td>The ARN of the agent.</td>
<td>System</td>
<td>$.Agent.ARN</td>
</tr>
</tbody>
</table>

**Note**

When you use an agent contact attribute in a **Transfer to agent** flow, the agent attributes reflect the target agent, not the one who initiated the transfer.

Agent attributes are available only in the following types of flows:

- Agent whisper
- Customer whisper
- Agent hold
- Customer hold
- Outbound whisper
- Transfer to agent. In this case, the agent attributes reflect the target agent, not the one who initiated the transfer.

Agent attributes are not available in the following flow types:

- Customer queue
- Transfer to queue
- Inbound flow

**Queue attributes**

These system attributes are returned when you use a **Get queue metrics** block in your flow.

If there is no current activity in your contact center, null values are returned for these attributes.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue name</td>
<td>The name of the queue for which metrics were retrieved.</td>
<td>System</td>
<td>$.Metrics.Queue.Name</td>
</tr>
<tr>
<td>Queue ARN</td>
<td>The ARN of the queue for which metrics were retrieved.</td>
<td>System</td>
<td>$.Metrics.Queue.ARN</td>
</tr>
<tr>
<td>Contacts in queue</td>
<td>The number of contacts currently in the queue.</td>
<td>System</td>
<td>$.Metrics.Queue.Size</td>
</tr>
<tr>
<td>Oldest contact in queue</td>
<td>For the contact that has been in the queue the longest, the length of time the contact has been in the queue, in seconds.</td>
<td>System</td>
<td>$.Metrics.Queue.OldestContactAge</td>
</tr>
<tr>
<td>Agents online</td>
<td>The number of agents currently online, which means logged in and in any state other than offline.</td>
<td>System</td>
<td>$.Metrics.Agents.Online.Count</td>
</tr>
<tr>
<td>Agents staffed</td>
<td>The number of agents currently staffed, which is</td>
<td>System</td>
<td>$.Metrics.Agents.Staffed.Count</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>agents logged in and in Available, ACW, or Busy states.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agents in After contact work</td>
<td>The number of agents currently in the ACW state.</td>
<td>System</td>
<td>$.Metrics.Agents.AfterContactWork.Count</td>
</tr>
<tr>
<td>Agents busy</td>
<td>The number of agents currently active on a contact.</td>
<td>System</td>
<td>$.Metrics.Agents.Busy.Count</td>
</tr>
<tr>
<td>Agents missed count</td>
<td>The number of agents in the Missed state, which is the state an agent enters after a missed contact.</td>
<td>System</td>
<td>$.Metrics.Agents.Missed.Count</td>
</tr>
</tbody>
</table>

**Telephony call metadata attributes (call attributes)**

Telephony metadata provides additional information related to call origination from telephony carriers.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Charge-Info</td>
<td>The party responsible for the charges</td>
<td>System</td>
<td>$.Media.Sip.Header.s.P-Charge-Info</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>--------------------</td>
</tr>
<tr>
<td>associated with the call</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>The identity of the end user associated with the request.</td>
<td>System</td>
<td>$.Media.Sip.Header.s.From</td>
</tr>
<tr>
<td>To</td>
<td>Information about the called party or the recipient of the request.</td>
<td>System</td>
<td>$.Media.Sip.Header.s.To</td>
</tr>
<tr>
<td>ISUP-OLI</td>
<td>Originating Line Indicator (OLI). Shows the type of line placing call (for example, PSTN, 800 service call, wireless/cellular PCS, payphone).</td>
<td>System</td>
<td>$.Media.Sip.Header.s.ISUP-OLI</td>
</tr>
<tr>
<td>Example value: 212555</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example value: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example value: 710</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Example value: 0235</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call-Forwarding-Indicator</td>
<td>Call Forwarding Indicators (for example, Diversion header). Indicates domestic or international origin of call.</td>
<td>System</td>
<td>$.Media.Sip.Header.s.Call-Forwarding-Indicator</td>
</tr>
<tr>
<td></td>
<td>Example value: sip:<a href="mailto:+15555555555@public-vip.us2.telephony-provider.com">+15555555555@public-vip.us2.telephony-provider.com</a>;reason=unconditional</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example value: 15555555555;noa=4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example value: 15555555555;noa=4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note

The availability of telephony metadata is not consistent across all telephony providers and may not be available in all cases. This may result in empty values.

Media streams attributes

The following table lists the attributes that you can use to identify the location in the live media stream where the customer audio starts and stops.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer audio stream ARN</td>
<td>The ARN of the Kinesis Video stream used for Live media streaming that includes the customer data to reference.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StreamARN</td>
</tr>
<tr>
<td>Customer audio stop timestamp</td>
<td>When the customer audio stream stopped the Kinesis video stream used for Live media streaming.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StopTimestamp</td>
</tr>
<tr>
<td>Customer audio start fragment number</td>
<td>The number that identifies the Kinesis Video Streams fragment, in the stream used for Live</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StartFragmentNumber</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alternate Intents</td>
<td>List of alternate intents available from Amazon Lex. Each intent has a corresponding confidence score and slots to fill.</td>
<td>Lex</td>
<td>$.Lex.AlternateIntentents.x.IntentName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.x.IntentConfidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.x.Slots</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.y.IntentName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.y.IntentConfidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.y.Slots</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.z.IntentName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.z.IntentConfidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.AlternateIntentents.z.Slots</td>
</tr>
</tbody>
</table>

**Amazon Lex contact attributes**

The following table lists the attributes that are returned from Amazon Lex bots.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intent Confidence</td>
<td>The intent confidence score returned by Amazon Lex.</td>
<td>Lex</td>
<td>$.Lex.IntentConfidence.Score</td>
</tr>
<tr>
<td>Score</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intent name</td>
<td>The user intent returned by Amazon Lex.</td>
<td>Lex</td>
<td>$.Lex.IntentName</td>
</tr>
<tr>
<td>Sentiment Label</td>
<td>The inferred sentiment that Amazon Comprehend has the highest confidence in.</td>
<td>Lex</td>
<td>$.Lex.SentimentResponse.Label</td>
</tr>
<tr>
<td>Sentiment scores</td>
<td>The likelihood that the sentiment was correctly inferred.</td>
<td>Lex</td>
<td>$.Lex.SentimentResponse.Scores.Positive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Lex.SentimentResponse.Scores.Negative</td>
</tr>
<tr>
<td>Session attributes</td>
<td>Map of key-value pairs representing the session-specific context information.</td>
<td>Lex</td>
<td>$.Lex.SessionAttributes.attributeKey</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Slots</td>
<td>Map of intent slots (key/value pairs) Amazon Lex detected from the user input during the interaction.</td>
<td>Lex</td>
<td>$.Lex.Slots.slotName</td>
</tr>
<tr>
<td>Dialog state</td>
<td>The last dialog state returned from an Amazon Lex bot. The value is 'Fulfilled' if an intent was returned to the flow.</td>
<td>N/A (no type appears in the UI)</td>
<td>$.Lex.DialogState</td>
</tr>
</tbody>
</table>

**Case contact attributes**

The following table lists the attributes that are used with Amazon Connect Cases.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
<th>Where the data comes from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case ID</td>
<td>Unique Identifier of the case in UUID format (for example, 689b0bea-aa29-4340-896d-4ca3ce9b6226)</td>
<td>text</td>
<td>$.Case.case_id</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Case Reason</td>
<td>The reason for opening the case</td>
<td>single-select</td>
<td>$.Case.case_reason</td>
<td>Agent</td>
</tr>
<tr>
<td>Customer</td>
<td>The API is a customer</td>
<td>text</td>
<td>$.Case.customer_id</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
<td>Where the data comes from</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Date/Time Closed</td>
<td>The date and time the case was last closed. It does not guarantee that a case is closed. If a case is reopened, this field contains the date/time stamp of the last time the status was changed to closed.</td>
<td>date-time</td>
<td>$.Case.last_closed_datetime</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Date/Time Opened</td>
<td>The date and time the case was opened.</td>
<td>date-time</td>
<td>$.Case.created_datetime</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Date/Time Updated</td>
<td>The date and time the case was last updated.</td>
<td>date-time</td>
<td>$.Case.last_updated_datetime</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
<td>Where the data comes from</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>-------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Reference number</td>
<td>A friendly number for the case in 8-digit numeric format.</td>
<td>text</td>
<td>$.Case.reference_number</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td>Reference numbers (unlike the Case ID) are not guaranteed to be unique.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>We recommend that you identify the customer and then collect the reference number to correctly find the right case.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the case</td>
<td>text</td>
<td>$.Case.status</td>
<td>Agent</td>
</tr>
<tr>
<td>Summary</td>
<td>Summary of the case</td>
<td>text</td>
<td>$.Case.summary</td>
<td>Agent</td>
</tr>
<tr>
<td>Title</td>
<td>Title of the case</td>
<td>text</td>
<td>$.Case.title</td>
<td>Agent</td>
</tr>
</tbody>
</table>

**Lambda contact attributes**

Lambda attributes are returned as key-value pairs from the most recent invocation of an `Invoke AWS Lambda function` block. External attributes are overwritten with each invocation of the Lambda function.

To reference external attributes in JSONPath, use:
• $.External.attributeName

where AttributeName is the attribute name, or the key of the key-value pair returned from the function.

For example, if the function returns a contact ID, reference the attribute with $.External.ContactId. When referencing a contact ID returned from Amazon Connect, the JSONPath is $.ContactId.

**Note**

Note the inclusion of `.External` in the JSONPath reference when the attribute is external to Amazon Connect. Make sure to match the case for attribute names returned from external sources.

For more information about using attributes in Lambda functions, see *Invoke AWS Lambda functions*.

These attributes are not included in contact records, not passed to the next Lambda invocation, and not passed to the CCP for screenpop information. However, they can be passed as Lambda function inputs on an *Invoke AWS Lambda function* block, or copied to user-defined attributes using the *Set contact attributes* block. When used in *Set contact attributes* blocks, the attributes that are copied are included in contact records, and can be used in the CCP.

**User-defined attributes**

For all other attributes Amazon Connect defines the key and value. For user-defined attributes, however, you provide a name for the key and the value.

Use user-defined attributes in situations where you want to store values in a contact flow, and then refer to those values later. For example, if you integrate Amazon Connect and a CRM or other system, you might want to get input from the customer such as their member number. Then you can use that member number retrieve information about the member from the CRM, and/or use the member number throughout the flow, etc.
To create user-defined attributes, use the Set contact attributes block.
Flow attributes

Flow attributes are like a type user-defined attribute, however, they are restricted to the flow where they are set.

Flow attributes are useful in situations where you don't want to persist the data throughout the contact, such as when you need to use sensitive information like the customer's credit card number to do a Lambda data dip.

- Flow attributes are temporary variables stored locally and only used in the flow. They aren't visible anywhere outside the flow, not even when the contact is transferred to another flow.
- They can be up to 32KB (the maximum size of the contact record attributes section).
- They aren't passed to a Lambda unless they are explicitly configured as parameters: in the Invoke AWS Lambda function block, choose Add a parameter.
- They aren't passed to modules. You can set a flow attribute within a module, but it won't be passed out of the module.
- They don't appear in the contact record.
- They don't appear to the agent in the CCP.
- The GetContactAttributes API can't expose them.
- If you have logging enabled on the flow, the key and value appear in the Cloudwatch log.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any name you choose</td>
<td>A flow attribute has two parts:</td>
<td>Flow</td>
<td>$.FlowAttributes.name_of_your_destination_key</td>
</tr>
<tr>
<td></td>
<td>• Destination key: this is any name you choose for the key. However, the $</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and . (period) characters are not allowed because they are both used in</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>defining the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>attribute paths in</td>
<td>attribute paths in JSONPath.</td>
<td>User-defined</td>
<td>$.Attributes.Messa</td>
</tr>
<tr>
<td>JSONPath.</td>
<td>• Value: this is can be any value you choose.</td>
<td></td>
<td>gingPlatform</td>
</tr>
<tr>
<td>MessagingPlatform</td>
<td>The messaging platform from where the customer request originated.</td>
<td>User-defined</td>
<td>$.Attributes.Messa</td>
</tr>
<tr>
<td>AppleBusinessChat</td>
<td>Exact value: <strong>AppleBusinessChat</strong></td>
<td></td>
<td>gingPlatform</td>
</tr>
<tr>
<td>CustomerId</td>
<td>The customer's opaque ID provided by Apple. This remains constant for the</td>
<td>User-defined</td>
<td>$.Attributes.Apple</td>
</tr>
<tr>
<td></td>
<td>AppleID and a business. You can use this to identify if the message is from</td>
<td></td>
<td>BusinessChatCustom</td>
</tr>
<tr>
<td></td>
<td>a new customer or a returning customer.</td>
<td></td>
<td>erId</td>
</tr>
</tbody>
</table>

**Apple Messages for Business attributes**

Use the following contact attributes to route Apple Business Chat customers. For example, if you have different lines of business using Apple Business Chat, you can branch to different flows based on the AppleBusinessChatGroup contact attribute. Or, if you want to route Apple Business Chat messages differently from other chat messages, you can branch based on MessagingPlatform.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppleBusinessChatIntent</td>
<td>You can define the intent or purpose of the chat. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the Business Chat button.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatIntent</td>
</tr>
<tr>
<td>AppleBusinessChatGroup</td>
<td>You define the group which designates the department or individuals best qualified to handle the customer’s particular question or problem. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the Business Chat button.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatGroup</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSON</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>AppleBusinessChatLocale</td>
<td>Defines the language and AWS Region preferences that the user wants to see in their user interface. It consists of a language identifier (ISO 639-1) and a Region identifier (ISO 3166). For example, en_US.</td>
<td>User-defined</td>
<td>$.Attributes.AppleBusinessChatLocale</td>
</tr>
<tr>
<td>AppleTimePickerCapability</td>
<td>Whether the customer device supports time pickers.</td>
<td>User-defined</td>
<td>$.Attributes.AppleTimePickerCapability</td>
</tr>
<tr>
<td></td>
<td>If true, customer device supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If false, their device does not supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppleListPickerCapability</td>
<td>Whether the customer device supports list pickers.</td>
<td>User-defined</td>
<td>$.Attributes.AppleListPickerCapability</td>
</tr>
<tr>
<td></td>
<td>If true, customer device supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If false, their device does not supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>AppleQuickReplyCapability</td>
<td>Whether the customer device supports quick replies. If true, customer device supports. If false, their device does not supports.</td>
<td>User-defined</td>
<td>$.Attributes.AppleQuickReplyCapability</td>
</tr>
</tbody>
</table>

**Customer Profiles attributes**

The following table lists the attributes that are used with Amazon Connect Customer Profiles.

The total size of Customer Profiles contact attributes is limited to 14,000 (56 attributes assuming max size of 255 each) characters for the entire flow. This includes all values persisted as Response fields in Customer Profiles blocks during the flow.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>profileSearchKey</td>
<td>The name of the attribute you want to use to search for a profile.</td>
<td>User-defined</td>
<td>Not applicable</td>
</tr>
<tr>
<td>profileSearchValue</td>
<td>The value of the key you want to search for, such as customer name or account number.</td>
<td>User-defined</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Profile ID</td>
<td>The unique identifier of a customer profile.</td>
<td>text</td>
<td>($.Customer.ProfileId)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Profile ARN</td>
<td>The ARN of a customer profile.</td>
<td>text</td>
<td>$.Customer.</td>
</tr>
<tr>
<td>First Name</td>
<td>The customer's first name.</td>
<td>text</td>
<td>$.Customer.FirstName</td>
</tr>
<tr>
<td>Middle Name</td>
<td>The customer's middle name.</td>
<td>text</td>
<td>$.Customer.MiddleName</td>
</tr>
<tr>
<td>Last Name</td>
<td>The customer's last name.</td>
<td>text</td>
<td>$.Customer.LastName</td>
</tr>
<tr>
<td>Account Number</td>
<td>A unique account number that you have given to the customer.</td>
<td>text</td>
<td>$.Customer.AccountNumber</td>
</tr>
<tr>
<td>Email Address</td>
<td>The customer's email address, which has not been specified as a personal or business address.</td>
<td>text</td>
<td>$.Customer.EmailAddress</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The customer's phone number, which has not been specified as a mobile, home, or business number.</td>
<td>text</td>
<td>$.Customer.PhoneNumber</td>
</tr>
<tr>
<td>Additional Information</td>
<td>Any additional information relevant to the customer's profile.</td>
<td>text</td>
<td>$.Customer.AdditionalInformation</td>
</tr>
<tr>
<td>Party Type</td>
<td>The customer's party type.</td>
<td>text</td>
<td>$.Customer.PartyType</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Business Name</td>
<td>The name of the customer's business.</td>
<td>text</td>
<td>$.Customer.BusinessName</td>
</tr>
<tr>
<td>Birth Date</td>
<td>The customer's birth date.</td>
<td>text</td>
<td>$.Customer.BirthDate</td>
</tr>
<tr>
<td>Gender</td>
<td>The customer's gender.</td>
<td>text</td>
<td>$.Customer.Gender</td>
</tr>
<tr>
<td>Mobile Phone Number</td>
<td>The customer's mobile phone number.</td>
<td>text</td>
<td>$.Customer.MobilePhoneNumber</td>
</tr>
<tr>
<td>Home Phone Number</td>
<td>The customer's home phone number.</td>
<td>text</td>
<td>$.Customer.HomePhoneNumber</td>
</tr>
<tr>
<td>Business Phone Number</td>
<td>The customer's business phone number.</td>
<td>text</td>
<td>$.Customer.BusinessPhoneNumber</td>
</tr>
<tr>
<td>Business Email Address</td>
<td>The customer's business email address.</td>
<td>text</td>
<td>$.Customer.BusinessEmailAddress</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Address</td>
<td>A generic address associated with the customer that is not mailing, shipping, or billing.</td>
<td>text</td>
<td>$.Customer.Address1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Address2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Address3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Address4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.City</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.County</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Country</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.PostalCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Province</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.State</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------</td>
<td>------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Shipping Address</td>
<td>The customer's shipping address.</td>
<td>text</td>
<td>$.Customer.ShippingAddress1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingAddress2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingAddress3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingAddress4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingCity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingCounty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingCountry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingPostalCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingProvince</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.ShippingState</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
<td>-------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Mailing Address</td>
<td>The customer's mailing address.</td>
<td>text</td>
<td>$.Customer.Mailing Address1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing Address2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing Address3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing Address4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing City</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing County</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing Country</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing PostalCode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing Province</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Mailing State</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------</td>
<td>------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Billing Address</td>
<td>The customer's billing address</td>
<td>text</td>
<td>$.Customer.Billing Address1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing Address2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing Address3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing Address4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing City</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing County</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing Province</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Billing State</td>
</tr>
<tr>
<td>Attributes</td>
<td>A key value pair of attributes of a customer profile.</td>
<td>text</td>
<td>$.Customer.Attributes.x</td>
</tr>
<tr>
<td>Object Attributes</td>
<td>A key value pair of custom object attributes of a customer profile.</td>
<td>text</td>
<td>$.Customer.ObjectAttributes.y</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Calculated Attributes</td>
<td>A key value pair of calculated attributes of a customer profile.</td>
<td>text</td>
<td>$.Customer.CalculatedAttributes.z</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------</td>
<td>-------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Asset</td>
<td>A customer's standard Asset.</td>
<td>text</td>
<td>$.Customer.Asset.AsssetId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.ProfileId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.AssetName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.SerialNumber</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.ModelNumber</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.ModelName</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.ProductSKU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.PurchaseDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.UsageEndDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.Quantity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Asset.Description</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>-----------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------</td>
<td>--------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Order</td>
<td>A customer's standard Order.</td>
<td>text</td>
<td>$.Customer.Order.OrderId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.ProfileId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.CustomerEmail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.CustomerPhone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.CreatedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.UpdatedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.ProcessedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.ClosedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.CancelledDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.CancelReason</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.AdditionalInformation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Order.Gateway</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>---------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>$.Customer.Order.TotalTipReceived</td>
<td></td>
<td></td>
<td>$.Customer.Order.TotalTipReceived</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>$.Customer.Order.ShippingName</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>$.Customer.Order.ShippingAddress1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingAddress2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingAddress3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingAddress4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingCity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingCounty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingCountry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingProvince</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.ShippingState</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.Customer.Order.Attributes.y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Case</td>
<td>A customer's standard Case.</td>
<td>text</td>
<td>$.Customer.Case.CaseId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.ProfileId</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.Title</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.CreatedBy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.CreatedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.UpdatedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.ClosedDate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.AdditionalInformation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.DataSource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$.Customer.Case.Attributes.z</td>
</tr>
</tbody>
</table>

List of attributes and their JSONPath reference
Outbound campaign attributes

You can use data in Amazon Pinpoint segments list to customize experiences in Amazon Connect flows. To reference data in a segment list, use Attributes_ColumnName. For more information, see Adding personalized content to message templates.

Note

Use $.Attributes.attributes_ColumnName to reference these attributes.

How to reference contact attributes

The way you reference contact attributes depends on how they were created and how you are accessing them.

• For the JSON syntax for each attribute, see List of available contact attributes and their JSONPath reference.
• To reference attributes that contain special characters in their name, such as spaces, place brackets and single quotations around the attribute name. For example: $.Attributes. ['user attribute name'].
• To reference attributes in the same namespace, such as a system attribute, you use the attribute name, or the name you specified as the Destination key.
• To reference values in a different namespace, such as referencing an external attribute, you specify the JSONPath syntax to the attribute.
• To use contact attributes to access other resources, set a user-defined attribute in your flow and use the Amazon Resource Name (ARN) of the resource you want to access as the value for the attribute.

Lambda examples

• To reference a customer name from a Lambda function lookup, use $.External.AttributeKey, replacing AttributeKey with the key (or name) of the attribute returned from the Lambda function.
• To use an Amazon Connect prompt in a Lambda function, set a user-defined attribute to the ARN for the prompt, and then access that attribute from the Lambda function.
Amazon Lex examples

- To reference an attribute from an Amazon Lex bot, you use the format $.Lex. and then include the part of the Amazon Lex bot to reference, such as $.Lex.IntentName.
- To reference the customer input to an Amazon Lex bot slot, use $.Lex.Slots.slotName, replacing slotName with the name of the slot in the bot.

Set contact attribute example

Use a Set contact attributes block to set a value that is later referenced in a flow. For example, create a personalized greeting for customers routed to a queue based on the type of customer account. You could also define an attribute for a company name or line of business to include in the text to speech strings said to a customer. The Set contact attributes block is useful for copying attributes retrieved from external sources to user-defined attributes.

To set a contact attribute with a Set contact attributes block

1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing flow, or create a new one.
3. Add a Set contact attributes block.
4. Edit the Set contact attributes block, and choose Use text.
5. For the Destination key, provide a name for the attribute, such as Company. This is the value you use for the Attribute field when using or referencing attributes in other blocks. For the Value, use your company name.

You can also choose to use an existing attribute as the basis for creating the new attribute.

Display contact information to the agent in the CCP

You can use contact attributes to capture information about the contact and then present it to the agent through the Contact Control Panel (CCP). For example, you might want to do this to customize the agent experience when using the CCP integrated with a customer relationship management (CRM) application.

Also use them when integrating Amazon Connect with a custom application using the Amazon Connect Streams API or Amazon Connect API. You can use all user-defined attributes, in addition
to the customer number and the dialed number, in the CCP using the Amazon Connect Streams JavaScript library. For more information, see Amazon Connect Streams API or Amazon Connect API.

When you use the Amazon Connect Streams API, you can access user-defined attributes by invoking contact.getAttributes(). You can access endpoints using contact.getConnections(), where a connection has a getEndpoint() invocation on it.

To access the attribute directly from a Lambda function, use $.External.AttributeName. If the attribute is stored to a user-defined attribute from a Set contact attributes block, use $.Attributes.AttributeName.

For example, included with your Amazon Connect instance, there is a flow named "Sample note for screenpop." In this flow, a Set contact attributes block is used to create an attribute from a text string. The text, as an attribute, can be passed to the CCP to display a note to an agent.

Route based on number of contacts in a queue

Amazon Connect includes queue attributes that can help you define routing conditions in your flows based on real-time metrics about the queues and agents in your contact center. For example, here are some common usage scenarios:

- Check the number of contacts or available agents in a queue, and how long the oldest contact has been in a queue, then route accordingly.

- To route to the queue with the fewest contacts in it:
  1. Get metrics for multiple queues.
  2. Use a Set contact attributes block to store the metric attributes for each queue.
  3. Compare queue metric attributes using a Check contact attributes block, and route the contact to the queue with the fewest calls in it, or to a callback if all queues are busy.

Using a Check contact attributes block to route a contact to a queue

1. In Amazon Connect, choose Routing, Contact flows.
2. Open an existing flow or create a new one.
3. Optionally, under Interact, add a Play prompt block to the designer to play a greeting to your customers. Add a connector between the Entry point block and the Play prompt block.
4. Under Set, drag a Get queue metrics block to the designer, and connect the Okay branch of the Play prompt block to it.
5. Choose the title of the **Get queue metrics** block to open the properties for the block. By default, the block retrieves metrics for the current working queue. To retrieve metrics for a different queue, choose **Set queue**.

6. Choose **Select a queue**, then select the queue to retrieve metrics for from the drop-down, then choose **Save**.

   You can also determine which queue to retrieve metrics for using contact attributes.

7. Under **Check**, drag a **Check contact attributes** block to the designer.

8. Choose the title of the block to display the settings for the block. Then, under **Attribute to check**, select **Queue metrics** in the **Type** drop-down menu.

9. Under **Attribute**, choose **Contacts in queue**.

10. To use conditions to route the contact, choose **Add another condition**.

    By default, the **Check contact attributes** block includes a single condition, **No match**. The **No match** branch is followed when there are no matches for any of the conditions you define in the block.

11. Under **Conditions to check**, select **Is less than** as the operator for the condition in the drop-down menu, then in the value field enter 5.

12. Choose **Add another condition**, then choose **Is greater or equal** from the drop-down menu, and enter 5 in the value field.

13. Choose **Save**.

   You now see two new output branches for the **Check contact attributes** block.

You can now add additional blocks to the flow to route the contact as desired. For example, connect the < 5 branch to a **Transfer to queue** block to transfer calls to the queue when there are fewer than five calls currently in the queue. Connect the > 5 branch to a Set customer callback number block and then transfer the call to a callback queue using a **Transfer to queue** block so the customer doesn't have to stay on hold.

**Route contacts based on queue metrics**

Many contact centers route customers based on the number of contacts waiting in a queue. This topic explains how to configure a flow that looks similar to the following image. It shows the following three flow blocks connected by Success branches: **Set contact attributes**, **Get queue metrics**, and **Check contact attributes**.
1. Add a **Set contact attributes** block to your flow.

2. In the **Set contact attributes**, specify the channel. If you set a channel dynamically using text, for the attribute value enter **Voice** or **Chat**, as shown in the following image. This value is not case-sensitive.

3. Add a **Get queue metrics** block to your flow.

In the Get queue metrics block, dynamic attributes can only return metrics for one channel.

**Add a Check contact attributes block after the Get queue metrics block**

After a **Get queue metrics** block, add a **Check contact attributes** block to branch based on the returned metrics. Use the following steps:
1. After Get queue metrics, add a Check contact attributes block.

2. In the Check contact attributes block, set Attribute to check to Queue metrics.

3. In the Attributes to check dropdown box, you'll see that the following queue metrics are returned by the Get queue metrics block. Choose the metric that you want to use for the routing decision.

4. Choose Add a condition to enter the comparison for your routing decision. The following image shows the block configured to check whether contacts in queue is greater than 5.
Route based on contact's channel

You can personalize the customer's experience based on the channel that they use to contact you. Here's what you do:

1. Add a Check contact attributes block to the beginning of your flow.

2. Configure the block as shown in the following image. In the Attribute to check section, set Type to System, set Attribute to Channel. In the Conditions to check section, set it to Equals CHAT.

3. The following image of the configured Check contact attributes block shows two branches: CHAT and No Match. If the customer is contacting you through chat, specify what should happen next. If the customer is contacting you through a call (No Match), specify the next step in the flow.
Use Amazon Lex and attributes

When you reference attributes in a Get customer input block, and choose Amazon Lex as the method of collecting the input, the attribute values are retrieved and stored from the output from the customer interaction with the Amazon Lex bot. You can use an attribute for each intent or slot used in the Amazon Lex bot, as well as the sessions attributes associated with the bot. An output branch is added to the block for each intent you include. When a customer chooses an intent when interacting with the bot, the branch associated with that intent is followed in the flow.

For a list of Amazon Lex attributes you can use and receive back from the Lex bot, see Amazon Lex contact attributes.

Using an Amazon Lex bot to get customer input

1. Open an existing or create a new flow.
2. Under Interact, drag a Get customer input block to the designer.
3. Choose the title of the block to display the block settings, then select Text to speech (Ad hoc).
4. Choose Enter text, then enter text in the Enter text to be spoken field that is used as a message or greeting to your customers. For example, "Thank you for calling" followed by a request to enter information to fulfill the intents you defined in your Amazon Lex bot.
5. Choose the Amazon Lex tab, then from the drop-down menu, choose the Amazon Lex bot to use to get customer input.
6. By default, the Alias field is populated with $LATEST. To use a different alias of the bot, enter the alias value to use.
Important

In a production environment, always use a different alias than TestBotAlias for Amazon Lex and $LATEST for Amazon Lex classic. TestBotAlias and $LATEST support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime quotas or Runtime Service Quotas (Amazon Lex Classic).

7. Optionally, to pass an attribute to Amazon Lex to use as a session attribute, choose Add an attribute. Specify the value to pass using either text or an attribute.

8. To create a branch from the block based on the customer intent, choose Add an intent, then enter the name of the intent exactly the same as the intent name in your bot.

9. Choose Save.

How to use Lex alternate intent attributes

Usually you configure flows to branch on the winning Lex intent. However, in some situations, you might want to branch on an alternate intent. That is, what the customer might have meant.

The following image shows the Properties page of the Check contact attributes block. It is configured to check a Lex attribute.

1. Intent name is the name of an alternate intent in Lex. It's case sensitive and must match what's in Lex exactly.
2. **Intent Attribute** is what Amazon Connect is going to check. In this example, it's going to check the **Intent Confidence Score**.

3. **Conditions to check**: If Lex is 70% certain the customer meant the alternate intent instead of the winning intent, branch.

### How to use Lex session attributes

When a customer starts a conversation with your bot, Amazon Lex creates a *session*. With *session attributes*, also known as *Lex attributes*, you can pass information between the bot and Amazon Connect during the session. For a list of Amazon Lex attributes you can use, see [Amazon Lex contact attributes](#).

### Life cycle of session attributes

There's one set of session attributes per conversation. In cases where a Lambda is invoked to do some processing, following is the order of precedence:

- **Service defaults**: these attributes are only used if no attributes are defined.
- **Session attributes provided by Amazon Connect**: these attributes are defined in the Get customer input block.
- **Session attributes provided by Lambda override everything prior**: When a Lambda function is invoked and it does some processing, it overrides any session attributes set in the Get customer input block.

Let's say a customer utters that they want a car. That's the first session attribute to go through processing. When asked what kind of car, they say luxury car, this second utterance overrides any Lambda processing that took place on the first utterance.

For an example of how to create a Lambda function that processes session attributes, see [Step 1: Create a Lambda Function](#) in the *Amazon Lex Developer Guide*. For information about Amazon Lex V2, see [Setting session attributes](#).

For the structure of the event data that Amazon Lex provides to a Lambda function, see [Lambda Function Input Event and Response Format](#) in the *Amazon Lex Developer Guide*. For information about Amazon Lex V2, see [Interpreting the input event format](#).

### Flow blocks that support Lex session attributes

You can use Lex session attributes in the following blocks when a Lex bot is called:
• Get customer input
• Set contact attributes
• Set hold flow
• Set working queue
• Set customer queue flow
• Set disconnect flow
• Set logging behavior
• Set callback number
• Set whisper flow
• Change routing priority/age
• Check contact attributes
• Loop
• Wait
• Invoke AWS Lambda function
• Transfer to phone number
• Transfer to flow

More information

For more information about using Amazon Lex session attributes, see Managing Conversation Context in the Amazon Lex Developer Guide.

How to use the same bot for voice and chat

You can use the same bot for both voice and chat. However, you may want the bot to respond differently based on the channel. For example, you want to return SSML for voice so a number is read as a phone number but you want to return normal text to chat. You can do this by passing the Channel attribute.

1. In the Get customer input block, choose the Amazon Lex tab.
2. Under Session attributes, choose Add an attribute. In the Destination key box, enter phoneNumber. Choose Set dynamically. In the Namespace box, choose System, and in the Value box, choose Customer Number, as shown in the following image.
3. Choose **Add an attribute** again.

4. Choose **Set dynamically**. In the **Destination key** box, enter **callType**. In the **Namespace** box, choose **System**, and in the **Value** box choose **Channel**, as shown in the following image.

5. Choose **Save**.

6. In your Lambda function, you can access this value in the **SessionAttributes** field in the incoming event.

### Lambda functions and attributes

Retrieve data from a system your organization uses internally, such as an ordering system or other database with a Lambda function, and store the values as attributes that can then be referenced in a flow.
When the Lambda function returns a response from your internal system, the response is key-value pairs of data. You can reference the values returned in the External namespace, for example $.External.attributeName. To use the attributes later in a flow, you can copy the key-value pairs to user-defined attributes using a **Set contact attributes** block. You can then define logic to branch your contact based on attribute values by using a **Check contact attributes** block. Any contact attribute retrieved from a Lambda function is overwritten with the next invocation of a Lambda function. Make sure you store external attributes if you want to reference them later in a flow.

**To store an external value from a Lambda function as a contact attribute**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. Select an existing flow, or create a new one.
3. Add an **Invoke AWS Lambda function** block, then choose the title of the block to open the settings for the block.
4. Add the **Function ARN** to your AWS Lambda function that retrieves customer data from your internal system.
5. After the **Invoke AWS Lambda function** block, add a **Set contact attributes** block and connect the **Success** branch of the **Invoke AWS Lambda function** block to it.
6. Edit the **Set contact attributes** block, and select **Use attribute**.
7. For **Destination key**, type a name to use as a reference to the attribute, such as `customerName`. This is the value you use in the **Attribute** field in other blocks to reference this attribute.
8. For **Type**, choose **External**.
9. For **Attribute**, enter the name of the attribute returned from the Lambda function. The name of the attribute returned from the function will vary depending on your internal system and the function you use.

After this block executes during a flow, the value is saved as a user-defined attribute with the name specified by the **Destination key**, in this case `customerName`. It can be accessed in any block that uses dynamic attributes.

To branch your flow based on the value of an external attribute, such as an account number, use a **Check contact attributes** block, and then add a condition to compare the value of the attribute to. Next, branch the flow based on the condition.
1. In the **Check contact attributes** block, for **Attribute to check** do one of the following:
   - Select **External** for the **Type**, then enter the key name returned from the Lambda function in the **Attribute** field.

   ![Important]
   
   Any attribute returned from an AWS Lambda function is overwritten with the next function invocation. To reference them later in a flow, store them as user-defined attributes.

   - Select **User Defined** for the **Type**, and in the **Attribute** field, type the name that you specified as the **Destination key** in the **Set contact attributes** block.

2. Choose **Add another condition**.

3. Under **Conditions to check**, choose the operator for the condition, then enter a value to compare to the attribute value. A branch is created for each comparison you enter, letting you route the contact based on the conditions specified. If no condition is matched, the contact takes the **No Match** branch from the block.

### Migrate flows to a different instance

Amazon Connect lets you efficiently migrate flows to another instance. For example, you might want to expand into new Regions, or move flows from your development environment to your production environment.

To migrate a few flows, use the [import/export feature](#) in the flow designer.

To migrate hundreds of flows, you need developer skills. You use the following procedure:

1. **Source instance**
   - **ListContactFlow**: Retrieve the Amazon Resource Number (ARN) for the flows that you want to migrate.
   - **DescribeContactFlow**: Get information about each flow that you want to migrate.

2. **Destination instance**
   - **CreateContactFlow**: Create the flows.
   - **UpdateContactFlowContent**: Update the flow content.
You must also build an ARN-to-ARN mapping for queues, flows, and prompts between the source and target Amazon Connect instances, and replace every ARN in the source flow with the corresponding ARN from the target instance. Otherwise UpdateContactFlowContent fails with InvalidContactFlow error.

You can update the information in the flows that you migrate. For more information, see Flow language in the Amazon Connect API Reference Guide.
Real-time and historical metrics dashboards and reports

In Amazon Connect, data about contacts are captured in contact records. This data can include the amount of time a contact spends in each state: customer on hold, customer in queue, agent interaction time.

The basis for most historical and real-time metrics in Amazon Connect is the data in the contact record. When you create metrics reports, the values displayed for most (not all) metrics in the report are calculated using the data in the contact records.

Contact records are available within your instance for 24 months from the time when the associated contact was initiated. You can also stream contact records to Amazon Kinesis to retain the data longer, and perform advanced analysis on it.

Tip
For detailed information about the activity of agents in your contact center, use Amazon Connect agent event streams.

Contents

- Dashboards
- Real-time metrics reports
- Historical metrics reports
- Login/Logout reports
- Amazon Connect agent event streams
- Amazon Connect contact events
- Contact records data model
- View a contact record in the UI
- About agent status
- About contact states
- About queued callbacks in metrics
- Save custom reports
Dashboards

Amazon Connect dashboards currently show real-time and historical metrics information and insights about your contact center performance. Real-time dashboards are updated every 15 seconds and you can select historical data as far back as 3 months in the past.

Data visualizations such as “Movers and shakers” display the largest changes compared to a custom-defined benchmark time period in the past (e.g., week over week), while “Contacts handled and average handle time trend” shows you the number of contacts handled alongside the average handle time over a period of intervals in time in a time series chart.

You can customize the dashboards (e.g. re-size and re-arrange the visuals), specify a custom time range and custom benchmark comparison time range for each dashboard, and select filters for data to include for each report. You can also download the entire data set or individual widgets as CSV, download the dashboard as a PDF, save your own version to your saved dashboards, share with individuals, and publish to the entire instance.

Topics

- Contact Lens conversational analytics dashboard
- Queue performance dashboard
- Required permissions

Contact Lens conversational analytics dashboard

With Amazon Connect Contact Lens, you can analyze conversations between customers and agents by using speech and chat transcriptions, natural language processing, and intelligent
search capabilities. Amazon Connect Contact Lens performs sentiment analysis, detects issues, and enables you to automatically categorize contacts. For more information, see Amazon Connect Contact Lens. With Amazon Connect Contact Lens, you can analyze conversations between customers and agents by using speech and chat transcriptions, natural language processing, and intelligent search capabilities. Amazon Connect Contact Lens performs sentiment analysis, detects issues, and enables you to automatically categorize contacts. For more information, see Analyze conversations using conversational analytics.

The Contact Lens conversation analytics dashboard helps you understand why end-customers are contacting, the trends of contact drivers over time, and the performance of each of those call drivers (e.g. average handle time for call driver “Where’s my stuff?”). You can view key metrics for categories like contacts handled and average handle time compared to a custom-defined benchmark time-range with color indicators (e.g. green = good, red = bad) for quick insights within seconds (e.g., “Am I performing better or worse than last week and by how much?”) using the summary widgets at the top. It has a drill-down ability into contacts in contact search to dive even deeper into performance insights. For example, within seconds you can use the dashboard to see a spike in contact volume, understand what is driving a spike in contact volume, and then click on a category driving the spike to take you to contact search pre-filtered for that category and dashboard filters (e.g. time range) to dig deeper into the individual contacts.

You can configure the dashboard by using the top-level dashboard filters to filter for individual or groups of agents, queues, routing profiles, channels, categories, and agent hierarchies. You will be able to look at contact categories trending up or down compared to a custom-defined benchmark time-range using the “Movers and shakers” widget. It has a configurable time-series widget where you can look at historical trends of count of contacts handled for any categories you want, going back as far as three months or as recent as the last 24 hours in 15 minute intervals. You can also use the time-series widget to see the performance of those calls (e.g. AHT) over time.

How to enable access to the Contact Lens conversational analytics dashboard

To enable access to the Contact Lens conversational analytics dashboard, you must first apply the appropriate Dashboard permission in the security profile, For more information, see Required permissions.

Next, you must also select Enable Contact Lens under Analytics tools in the AWS console.
To see data in your dashboard, you must have the **Contact Lens - conversational analytics** permission checked in the security profile.

Lastly, you must apply Contact Lens conversational analytics to your Flow in order to have Contact Lens analyze your contacts. See [Enable Amazon Connect Contact Lens](#).

**How does the dashboard work?**

The following sections walks you through the dashboard from top to bottom.

**How to get to the dashboard?**

Under **Analytics and Optimization**, choose **Dashboards and reports**. Then choose **Select** under **Conversational analytics dashboard** in the **Dashboards** section. The dashboards you can select are Connect pre-built dashboards that you can configure and save as your own dashboard to appear in the **My dashboards** section below it. See the next section for more details.
Dashboard actions

1. Save: You can save your dashboard and change your dashboard name by clicking “Actions” > “Save” and typing a new name and clicking “Save.” Your saved dashboard will appear in your “Saved dashboards” in the “Dashboards and reports” page within the “Dashboards” tab.

2. Save as: You can re-name and save your dashboard by clicking “Actions” > “Save as” and typing a new name and clicking save. Your saved dashboard will appear in your “Saved dashboards” in the “Dashboards and reports” page within the “Dashboards” tab.

3. Download CSV: You can download the entire dashboard data set to CSV by clicking “Actions” > “Download CSV.” You can also download each widget’s data set individually by clicking the download arrow button in the top right of each widget.

4. Download PDF: You can download the entire dashboard as a PDF by clicking “Actions” > “Download PDF.”

5. Share: You can share and publish the dashboard like other Connect reports by clicking “Actions” > “Share.” For more information about sharing and publishing, see Share reports, View shared reports, and Publishing reports.
Other actions: You can move charts around by clicking and holding the top left corner icon with your mouse and moving. You can re-size widgets by clicking and dragging the bottom right icon with your mouse.

Filters

You can configure your dashboard with the following filters:

Required filters:

1. Time range: You can select a real-time time range within the “Time range: Today” option and choose a trailing window of time. For additional windows, select “Custom.” You can select historical time ranges by altering your Time range to “Day,” “Week,” or “Month.”

2. “Compare to” benchmark time range: You can customize a comparison time period to benchmark your Time range selection against, such as an exact week over week comparison called “Compare to: Prior week same day, time range, and time.” This benchmark time range powers the benchmarking in all of the widgets in the dashboard. Your benchmark time range must be a date in the past compared to your time range.
Additional filters: Contact Category, Agent, Queue, Channel, Routing Profile, and Agent Hierarchy.

Performance overview charts

There are two performance overview charts that provide aggregated metrics based on your filters. The second chart is further filtered only by contacts analyzed by Contact Lens conversational analytics. Each metric within the charts is compared to your “compare to” benchmark time range filter. For example, Contacts handled during your time range selection was 165,522, which is down ~12% compared to your benchmark number of contacts handled, 187,949 contacts. The percentages are rounded up or down. The colors that appear for the metrics indicate positive (green) or negative (red) compared to your benchmark. There are no colors for contacts handled.
Contact categories

The contact categories chart shows you Contact Category information. To see all data, click on the pop-out icon in the top right of the chart. To deep dive further into the contacts, click on the Contact Category and it will take you to Contact Search pre-filtered for that category along with the dashboard filters.

1. Contacts %: the count of contacts analyzed by Contact Lens conversational analytics that have a given category divided by the total number of contacts analyzed by Contact Lens conversational analytics.
2. Contacts: count of contacts analyzed by Contact Lens conversational analytics that have a given category.
3. AHT: the average handle time for the contacts that have a given category.
4. Avg. queue answer time: the average queue answer time for the contacts that have a given category.
5. Contacts transferred in: the count of contacts transferred in for the contacts that have a given category.

Movers and shakers

The movers and shakers chart shows you the categories with the highest percent change in distribution compared to your benchmark time range. In other words, it shows you the count of categories that were generated more or less frequently compared to the total number of contacts analyzed by Contact Lens conversational analytics. For example, if 20 out of 100 contacts analyzed by Contact Lens have Category A, your contacts % for Category A was 20%. If during the comparison benchmark time period 10 out of 100 contacts analyzed by Contact Lens
conversational analytics had Category A, your Prior contacts % for Category A was 10%. The % Change would be \((20\% - 10\%)/(10\%) = 100\%\). To see all data, click on the pop-out icon in the top right of the chart. To deep dive further into the contacts, click on the Contact Category and it will take you to Contact Search pre-filtered for that category along with the dashboard filters.

1. Change %: \((\text{Contacts } \% - \text{Prior contacts } \%)/\text{(Prior contacts } \%\)\). This number is rounded. The chart is sorted by highest absolute Change %.

2. Contacts %: the count of contacts analyzed by Contact Lens conversational analytics in the time range specified in your dashboard filter that have a given category divided by the total number of contacts analyzed by Contact Lens conversational analytics.

3. Contacts: the count of contacts analyzed by Contact Lens conversational analytics in the time range specified in your dashboard filter.

4. Prior contacts %: the count of contacts analyzed by Contact Lens conversational analytics in the “compare to” benchmark time range specified in your dashboard filter that have a given category divided by the total number of contacts analyzed by Contact Lens conversational analytics.

5. Prior contacts: the count of contacts analyzed by Contact Lens conversational analytics in the “compare to” benchmark time range specified in your dashboard filter.

Top contact categories average handle time

The top contact categories average handle time displays the prior AHT (using the “compare to” benchmark time range) to the current time range AHT for each of your top 10 categories (sorted by count of contacts with a category from left to right). To see all data, click on the pop-out icon in the top right of the chart.
Contact count by queue

The contact count by queue chart displays the count of contacts for each queue, sorted by the highest number of contacts from left to right. You can configure this widget further by filtering for contact categories directly from this chart. This filter will override the page-level contact category filter at the top of the dashboard.

Contacts handled and average handle time trend

The Contacts handled and average handle time trend is a time-series chart that displays the count of contacts handled (blue bars) and the average handle time (red line) over a given time period.
broken down by intervals (15min, daily, weekly, monthly). You can configure different time range intervals by using the “Interval” button directly in the widget. The intervals that you may select depend on the page-level time range filter. For example, if you have a “Today” time range filter at the top of your dashboard, you can only see an interval of 15min for the last 24 hours. If you have a “Day” time range filter at the top of your dashboard, you can see a trailing 8 day interval trend, or a 15min interval trend for the trailing 24 hours.

Dashboard functionality limitations

The following limitations apply to the Contact Lens conversational analytics dashboard:

1. Tag-based access controls are not enforced on the dashboard.

2. If you have a routing profile or agent hierarchy filter selected, the hyperlinks on contact categories leading to contact search will be disabled within the Contact categories and Movers and Shakers charts.

Queue performance dashboard

The queue performance dashboard helps you understand the performance of your queues or groups of queues compared over configurable periods of time using key metrics such as contacts handled, service level, and average handle time.
How to enable access to the queue performance dashboard

To enable access to the queue performance dashboard, you must apply the appropriate Dashboard permission in the security profile. For more information, see Required permissions.

How to get to the dashboard?

Under Analytics and Optimization, choose Dashboards and reports. Then choose Select under Queue performance dashboard in the Dashboards section. The dashboards you can select are Connect pre-built dashboards that you can configure and save as your own dashboard to appear in the My dashboards section below it. See the next section for more details.

Dashboard Actions

1. Save: You can save your dashboard and change your dashboard name by clicking “Actions” > “Save” and typing a new name and clicking “Save.” Your saved dashboard will appear in your “Saved dashboards” in the “Dashboards and reports” page within the “Dashboards” tab.

2. Save as: You can re-name and save your dashboard by clicking “Actions” > “Save as” and typing a new name and clicking save. Your saved dashboard will appear in your “Saved dashboards” in the “Dashboards and reports” page within the “Dashboards” tab.
3. Download CSV: You can download the entire dashboard data set to CSV by clicking “Actions” > “Download CSV.” You can also download each widget’s data set individually by clicking the download arrow button in the top right of each widget.

4. Download PDF: You can download the entire dashboard as a PDF by clicking “Actions” > “Download PDF.”

5. Share: You can share and publish the dashboard like other Connect reports by clicking “Actions” > “Share.” For more information about sharing and publishing, see Share reports, View shared reports, and Publishing reports.

Other actions: You can move charts around by clicking and holding the top left corner icon with your mouse and moving. You can re-size widgets by clicking and dragging the bottom right icon with your mouse.

Filters

You can configure your dashboard with the following filters:
Required filters:

1. Time range: You can select a real-time time range within the “Time range: Today” option and choose a trailing window of time. For additional windows, select “Custom.” You can select historical time ranges by altering your Time range to “Day,” “Week,” or “Month.”

2. “Compare to” benchmark time range: You can customize a comparison time period to benchmark your Time range selection against, such as an exact week over week comparison called “Compare to: Prior week same day, time range, and time.” This benchmark time range powers the benchmarking in all of the widgets in the dashboard. Your benchmark time range must be a date in the past compared to your time range.

Additional filters: Agent, Queue, Channel, Routing Profile, Agent and Hierarchy.

Performance overview chart

The performance overview chart that provides aggregated metrics based on your filters. Each metric within the charts is compared to your “compare to” benchmark time range filter. For example, Contacts handled during your time range selection was 126,306, which is down ~13% compared to your benchmark number of contacts handled, 144,647 contacts. The percentages are rounded up or down. The colors that appear for the metrics indicate positive (green) or negative (red) compared to your benchmark. There are no colors for contacts handled.
Contacts handled and average handle time trend

The Contacts handled and average handle time trend is a time-series chart that displays the count of contacts handled (blue bars) and the average handle time (red line) over a given time period broken down by intervals (15min, daily, weekly, monthly). You can configure different time range intervals by using the “Interval” button directly in the widget. The intervals that you may select depend on the page-level time range filter. For example, if you have a “Today” time range filter at the top of your dashboard, you can only see an interval of 15min for the last 24 hours. If you have a “Day” time range filter at the top of your dashboard, you can see a trailing 8 day interval trend, or a 15min interval trend for the trailing 24 hours.
Dashboard functionality limitations

The following limitations apply to the Contact Lens conversational analytics dashboard:

1. Tag-based access controls are not enforced on the dashboard.

Required permissions

To view dashboards, you need to be assigned to a security profile that has either the Access metrics – Access permission or the Dashboards – Access permission. Note the following behavior when you assign these permissions:

1. When Access metrics – Access is selected, the Real-time metrics, Historical metrics, Agent activity audit, and Dashboards permissions are also automatically assigned.

2. When Access metrics – Access is assigned, you have access to all real-time and historical metrics reports and dashboards.

The following image shows the Analytics and Optimization section of the Security profile permissions page. The Access option is selected for Access metrics, Real-time metrics, Historical metrics, Agent activity audit, and Dashboards.
If only **Dashboards** is selected, you have access only to dashboards and no other analytics pages or reports. The following image shows the **Analytics and Optimization** section, with only **Dashboards – Access** selected.

### Real-time metrics reports

Real-time metrics reports show real-time or near-real time metrics information about activity in your contact center. Metrics such as **Online** show the number of agents currently online in real-time, updating every 15 seconds. Metrics such as **Handled** and **Abandoned** reflect near real-time values for your contact center.

You can customize the reports, specify a time range for each report, select metrics for each report, and select filters for data to include or exclude from each report.

You can also use the [Amazon Connect Service APIs](https://aws.amazon.com/connect/service-api/) to create custom reports, such as real-time reports that are filtered by teams of agents.

**Contents**

- Real-time metrics definitions
- Permissions required to view real-time metrics reports
• **Real-time metrics tag-based access control**
• **How often real-time metrics refresh**
• **Use one-click drill-downs for Routing profiles and Queues tables**
• **Visualize: Queue dashboard**
• **View how many contacts are waiting in queue**
• **Create a real-time metrics report**
• **No metrics or too few rows in a queues report?**
• **List queues grouped by routing profile**
• **List agents grouped by routing profile**
• **Sort agents by activity in a real-time metrics report**
• **Change the "Agent activity" status in a real-time metrics report**
• **Download a real-time metrics report**

**Real-time metrics definitions**

The following metrics are available to include in real-time metrics reports in Amazon Connect. The metrics available to include in a report depend on the report type.

⚠️ **Tip**

Developers can use the [GetCurrentMetricData](#) API to get a subset of the following real-time metrics from the specified Amazon Connect instance.

---

**Abandoned**

The count of contacts disconnected by the customer while in the queue during the specified time range. Contacts queued for callback are not counted as abandoned. When you create a customized real-time metrics report, to include this metric, choose a **Queues** report for the type. On the **Filters** tab, choose **Queues**, then on the **Metrics** tab you'll have the option to include **Abandoned**.

**Active**

The count of active slots. This number is incremented for each contact where the contact state is either Connected, On Hold, After contact work, or Outbound ring.
In the `GetCurrentMetricData` API, this metric can be retrieved by using `SLOTS_ACTIVE`.

**ACW**

The count of contacts that are in an `AfterContactWork` state. (After contact work is also known as After call work.) After a conversation between an agent and customer ends, the contact is moved into the ACW state.

In the `GetCurrentMetricData` API, this metric can be retrieved by using `AGENTS_AFTER_CONTACT_WORK`. The name of this metric is confusing because in the Amazon Connect console, ACW counts the number of contacts that are in an ACW state, not the number of agents.

To learn more about agent status and contact states, see [About agent status](#) and [About contact states](#).

**Agent Activity**

If an agent is handling a single contact, this metric may have the following values: Available, Incoming, On contact, Rejected, Missed, Error, After contact work, or a custom status.

If an agent is handling concurrent contacts, Amazon Connect uses the following logic to determine the state:

- If at least one contact is in Error, Agent Activity = Error.
- Else if at least one contact is Missed contact, Agent Activity = Missed.
- Else if at least one contact is Rejected contact, Agent Activity = Rejected.
- Else if at least one contact is Connected, On Hold, or Outbound contact/Outbound callback, Agent Activity = On contact.
- Else if at least one contact is After contact work, Agent Activity = After Contact Work.
- Else if at least one contact is Incoming/Inbound Callback, Agent Activity = Incoming.
- Else if agent status is a custom status, Agent Activity is the custom status.
- Else if agent status is Available, Agent Activity = Available.

If a manager is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, then the manager's Agent Activity will display as Monitoring. The Agent Activity of the agent who is being monitored is still On Contact.
Agent First Name

The first name of the agent, as entered in their Amazon Connect user account.

Agent Hierarchy

The hierarchy the agent is assigned to, if any.

Agent hung up

The count of contacts disconnected where the agent disconnected before the customer.

Agent Last Name

The last name of the agent, as entered in their Amazon Connect user account.

Agent Name

The name of the agent, displayed as follows: Agent Last Name, Agent First Name.

Agent non-response

The count of contacts routed to an agent but not answered by that agent, including contacts abandoned by the customer.

If a contact is not answered by a given agent, we attempt to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times (including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

This metric was previously named Missed.

AHT (Average Handled Time)

The average time, from start to finish, that a contact was connected with an agent (average handled time). It includes talk time, hold time, and After Contact Work (ACW) time.

AHT is calculated by averaging the amount of time between the contact being answered by an agent and the completion of work on that contact by an agent.
API contacts handled

The count of contacts that were initiated by an API operation, such as StartOutboundVoiceContact, and handled by an agent.

Availability

For each agent, the number of available slots they have that can be routed contacts.

The number of available slots for an agent are based on their routing profile. For example, let's say an agent's routing profile specifies they can handle either one voice contact or up to three chat contacts simultaneously. If they are currently handling one chat, they have two available slots left, not three.

What causes this number to go down? A slot is considered unavailable when:

- A contact in the slot is: connected to the agent, in After Contact Work, inbound ringing, outbound ringing, missed, or in an error state.
- A contact in the slot is connected to the agent and on hold.

Amazon Connect doesn't count an agent's slots when:

- The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.
- The agent can't take contacts from that channel per their routing profile.

In the GetCurrentMetricData API, this metric can be retrieved by using SLOTSAVAILABLE.

Available

The number of agents who can take an inbound contact. An agent can only take inbound contacts when they manually set their status to Available in the CCP (or in some cases when their manager changes it).

This is different from how many more inbound contacts an agent could take. If you want to know how many more contacts an agent can have routed to them, look at the Availability metric. It indicates how many slots the agent has free.
What causes this number to go down? An agent is considered **unavailable** when:

- The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.
- The agent has at least one contact ongoing.
- The agent has a contact in a missed or error state, which prevents the agent from taking any more contacts until they are flipped back to routable.

In the [GetCurrentMetricData](#) API, this metric can be retrieved by using AGENTS_AVAILABLE.

**Average API Connecting Time**

The average time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

**Avg abandon time**

Average time, in seconds, that abandoned contacts were in the queue before being abandoned.

**Avg ACW**

Average time, in seconds, that contacts spent in the **After contact work** state, during the specified time range.

This is not the average amount of time agents spent on contacts.

To learn more about agent status and contact states, see [About agent status](#) and [About contact states](#).

**Avg callback connecting time**

The average time between when callback contacts are initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the five parts that go into calculating **Avg callback connecting time**: Amazon Connect assign work item to agent, agent accepts work item, connection build time, network connection time, rings for customer. It also shows what is in the agent event stream: Connecting, Connected or no answer.
Avg hold time

Average time, in seconds, that a contact in the queue was on hold.

This metric doesn't apply to tasks so you'll notice a value of 0 on the report for them.

Avg incoming connecting time

The average time between when contacts are initiated Amazon Connect reserving the agent for the contact, and the agent is connected.

In the agent event stream, this time is calculated by averaging the duration between the contact state of STATE_CHANGE event changes from CONNECTING to CONNECTED/MISSED/ERROR.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the three parts that go into calculating Avg incoming connecting time: connection build time, network connection time, and requesting agent to accept. It also shows what is in the agent event stream: Connecting, Connected, Missed, or Rejected.
**Avg interaction time**

Average time, in seconds, that contacts were connected to and interacting with agents. This does not include hold time or time spent waiting in the queue.

**Avg interaction and hold time**

Average time, in seconds, that contacts in the queue spent interacting with agents and on hold. This is calculated as follows:

Avg hold time + Avg interaction time

**Avg queue answer time**

Average time, in seconds, that a contact was in the queue before being answered by an agent. This is calculated using the amount of time that the contact was in the queue, not any time that the contact spent in prior steps of the flow, such as listening or responding to prompts.

**Avg outbound connecting time**

The average time between when outbound contacts are initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the four parts that go into calculating Avg outbound connecting time: agent call customer, connection build time, network connection time, rings for customer. It also shows what is in the agent event stream: Connecting, Connected or No answer.
Callback contacts handled

The count of contacts handled by an agent that were queued callbacks.

Capacity

Displays the maximum capacity that's set in the routing profile currently assigned to the agent. This column can be filtered by channel.

If an agent's routing profile is configured to handle either one voice or up to three chats, then their maximum capacity equals three, when not filtered by channel.

Consult

Deprecated May 2019. When used in a report, it returns a dash (-).

The count of contacts in the queue that were handled by an agent, and the agent consulted with another agent or a call center manager during the contact.

Contact State

The state of the contacts the agent is currently handling. The state can be: Connected, On Hold, After contact work, Incoming, Calling, or Missed contact.

For queued callbacks, the contact state can also Callback incoming or Callback dialing.

If a manager is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, the manager's contact state is Monitoring; the agent's contact state is Connected.

Contacts Abandoned in X

The number of contacts abandoned between 0 and X, for example, from 0 - 60 seconds.

You can create custom thresholds for contacts abandoned. For more information, Custom service levels.

Custom contacts abandoned is localized to the report where the metric is applied. For example, you create a report that has a Contacts abandoned in 75 seconds metric. You leave the page and then create another report. The Contacts abandoned in 75 seconds metric won't exist in the second report. You'll need to create it again.
Contacts Answered in X

The number of contacts answered between 0 and X, for example, from 0 - 60 seconds.

You can create custom thresholds for contacts answered. For more information, Custom service levels.

Custom contacts answered is localized to the report where the metric is applied. For example, you create a report that has a Contacts answered in 75 seconds metric. You leave the page and then create another report. The Contacts answered in 75 seconds metric won't exist in the second report. You'll need to create it again.

Duration

Amount of time that the agent has been in the current Agent Activity State.

Error

A count of agents in Error state. An agent is included in this metric if they miss a call or reject a chat/task (most common). They could also be counted if there is a connection failure.

In the GetCurrentMetricData API, this metric can be retrieved by using AGENTS_ERROR.

Handled

The count of contacts in the queue that were answered by an agent.

Handled in

The count of incoming contacts handled by an agent during the specified time range that were initiated using one of the following methods: inbound call, transfer to agent, transfer to queue, or queue-to-queue transfer.

Handled out

The count of contacts handled by an agent during the specified time range that were initiated by an agent placing an outbound call using the CCP.

Hold abandons

The count of contacts that disconnected while the customer was on hold. A disconnect could be because the customer hung up while on hold, or that there was a technical issue with the contact while on hold.
In queue

The count of contacts currently in the queue.

To learn how this is different from Scheduled contacts in a callback scenario, see How Initial delay affects Scheduled and In queue metrics.

In the GetCurrentMetricData API, this metric can be retrieved by using CONTACTS_IN_QUEUE.

Max queued

The longest time that a contact spent waiting in the queue. This includes all contacts added to the queue, even if they were not connected with an agent, such as abandoned contacts.

NPT (Non-Productive Time)

The count of agents who have set their status in the CCP to a custom status. That is, their CCP status is other than Available or Offline.

Tip

Although agents aren't routed any new inbound contacts while their CCP status is set to a custom status, it's possible for them to change their CCP status to a custom status while still handling a contact. For example, let's say an agent is being routed contacts very quickly. To go on break, they set their status to Break proactively, while still finishing up the last contact. This allows them to go on break and avoid accidentally missing a contact that's routed to them in the sliver of time between the last contact ending and setting their status to Break.

Because agents can be On call or doing ACW, for example, while their CCP is set to a custom status, this means it's possible for agents to be counted as On call and NPT at the same time.

In the GetCurrentMetricData API, this metric can be retrieved by using AGENTS_NON_PRODUCTIVE.

Occupancy

Percentage of time that an agent was active on contacts. This percentage is calculated as follows:

\[
\frac{(\text{Agent on contact (wall clock time)})}{(\text{Agent on contact (wall clock time)} + \text{Agent idle time})}
\]
Where:

- \((\text{Agent on contact} + \text{Agent idle time}) = \text{total amount of agent time}\)
- \(\frac{\text{Agent on contact}}{\text{total amount of agent time}} = \text{percentage of time agents were active on contacts}\).

**Important**

*Occupancy* doesn't account for concurrency. That is, an agent is considered 100% occupied for a given interval if they are handling at least one contact for that entire duration.

**Oldest**

Length of time in the queue for the contact that has been in the queue the longest.

In the [GetCurrentMetricData](#) API, this metric can be retrieved by using `OLDEST_CONTACT_AGE`.

**On contact**

The count of agents currently on a contact. An agent is "on a contact" when they are handling at least one contact that is either connected, on hold, in After contact work, or outbound ring.

In the [GetCurrentMetricData](#) API, this metric can be retrieved by using `AGENTS_ON_CONTACT`. This metric used to be named On call. You can still use `AGENTS_ON_CALL` to retrieve data for this metric.

**Online**

The count of agents who have set their status in the CCP to something other than *Available*. For example, they may have set their status to Available, or to a custom value such as Break or Training.

The Online metric doesn't tell you how many agents can be routed contacts. For that metric, see [Available](#).

This metric can be confusing so let's look at an example. Say you see this in a Queues report:

- Online = 30
• On Call = 1
• NPT = 30
• ACW = 0
• Error = 0
• Available = 0

This means 30 agents have set their status in the CCP to a custom status. 1 of those 30 agents is currently on a contact.

In the GetCurrentMetricData API, this metric can be retrieved by using AGENTS_ONLINE.

**Queue**

The name of the queue associated with the contact the agent is currently handling.

**Queued**

The count of contacts added to the queue during the specified time range.

**Routing Profile**

The routing profile for the agent.

**Scheduled**

The count of customers in the queue for which there is a callback scheduled.

To learn how this is different from In queue contacts in a callback scenario, see How Initial delay affects Scheduled and In queue metrics.

In the GetCurrentMetricData API, this metric can be retrieved by using CONTACTS_SCHEDULED.

**SL X**

Percentage of contacts removed from the queue between 0 and X after being added to it (Service Level). A contact is removed from the queue when one of the following occurs: an agent answers the call, the customer abandons the call, or the customer requests a call back.

For X, you can choose from pre-set times in seconds: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.
Custom service levels

You can also create custom service level metrics. You can also choose from additional durations, such as minutes, hours, or days.

You can add up to 10 custom service levels per report.

The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

Staffed

The count of agents who are online in the CCP, and not in NPT (a custom status).

Another way of thinking about this is, there are two scenarios in which Staffed is not incremented:

- The agent's status in the CCP is set to Offline.
- The agent's status in the CCP is set to a custom status.

For example, let's say an agent sets their status in the CCP to a custom status such as Break and they make an outbound call. Now the agent is On call, but Staffed is 0.

If the agent sets their status in the CCP to Available and makes an outbound call, the agent is On call and Staffed is 1.

This metric is available on the Queues report.

In the GetCurrentMetricData API, this metric can be retrieved by using AGENTS_STAFFED.

Transferred in

The count of contacts transferred into the queue during the specified time range.

Transferred in by agent

The count of contacts transferred in by an agent using the CCP.

Transferred in from queue

The count of contacts transferred into the queue from another queue during a Customer queue flow.
Transferred out

The count of contacts transferred out of the queue during the specified time range.

Transferred out by agent

The count of contacts transferred out by an agent using the CCP.

Transferred out from queue

The count of contacts transferred out of the queue to another queue during a Customer queue flow.

Permissions required to view real-time metrics reports

To view real-time metrics reports, you need to be assigned to a security profile that has either the Access metrics - Access permission or the Real-time metrics - Access permission. Note the following behavior when you assign these permissions:

- When Access metrics - Access is selected, the Real-time metrics, Historical metrics, and Agent activity audit permissions are also automatically assigned.
- When Access metrics - Access is assigned, you have access to all real-time and historical metrics reports.

The following image shows the Analytics and Optimization section of the Security profile permissions page. The Access option is selected for Access metrics, Real-time metrics, Historical metrics, and Agent activity audit.

If only Real-time metrics is selected, you have access only to real-time metrics and no other analytics pages or reports. The following image shows the Analytics and Optimization section, with only Real-time metrics - Access selected.
Real-time metrics tag-based access control

You can use resource tags and access control tags to apply granular access to users, queues, and routing profiles for real-time metrics. For example, you can control who has access to view specific users, queues, and routing profiles on the Real-time metrics page.

Without tag-based access controls, all queues, routing profiles, and agents appear on the Real-time metrics page, as shown in the following image.

With tag-based access controls, a limited set of queues, routing profiles, and agents appear on the Real-time metrics page, as shown in the following image.
Tag-based access controls enable you to configure granular access to specific resources based on assigned resource tags. You can configure tag based access controls by using the API/SDK or within the Amazon Connect console (for supported resources). You must configure user resource tags and access control tags before tag-based access control is applied to users for the agent activity audit report. For more information, see [Tagging resources in Amazon Connect](#) and [Tag-based access control](#).

**How to enable tag-based access control for real-time metrics**

To use tags to control access to users, queues, and routing profiles for real-time metrics, you must first configure resource tags and access control tags. For more information, see [Tagging resources in Amazon Connect](#) and [Tag-based access control](#).

After your resource tags and access control tags are configured, you must apply the appropriate permissions. When your resource tags, access control tags, and permissions have been appropriately configured, you will have access controls applied to users, queues, and routing profiles for real-time metrics.

**Permissions**

To view real-time metrics reports that have tag-based access controls applied to them, you need to be assigned to a security profile that has permissions to:

- Access metrics.
- Access the resources you want to view, such as routing profiles and queues.
Permissions to access metrics

You need one of the following Analytics and Optimization security profile permissions:

- **Access metrics - Access**
- **Real-time metrics - Access**, as shown in the following image of the Analytics and Optimization section of the security profiles page.

When you enable **Access metrics - Access**, permissions are also automatically granted to **Real-time metrics**, **Historical metrics**, and **Agent activity audit**. The following image shows all of these permissions granted.

### Note

When users have all of these permissions, they can see all data for historical metrics for which tag-based access controls are not currently applied.
Permissions to access resources

The following image shows an example of security profile permissions that grant users the ability to view routing profiles, queues, and Amazon Connect user accounts. **Routing profiles - View**, **Queues - View**, and **Users - View** are selected.

Functionality limitations

The following limitations apply to tag-based access controls for real-time metrics.

1. You can only filter and group tables by the primary resource (user, queue, or routing profile).
   You cannot filter and group tables by non-primary resources. For example, you cannot filter by queue in an agent table and you cannot group by queue in a routing profile table.
2. Drill-down button disabled within tables except for View queue graphs. For example, you cannot choose View agents in a queue table.

3. Access to the homepage service level dashboard is disabled.

4. Access to view Agent Queues is disabled.

5. Agent Adherence table is not yet supported.

**Transitioning to tag-based access control**

If you open a saved report containing tables with users, queues, or routing profiles that you don't have access to anymore due to tag-based access control, or if groupings or non-primary filters are applied to tables, you won't see data in those tables.

To view the data, do one of the following steps:

- Edit your table filters to include the agents, queues, or routing profiles that you have access to.
- Create a new report that includes the resources you have access to.
- Remove the groupings and non-primary filters from the table.

**How often real-time metrics refresh**

Data in real-time metrics reports is refreshed as follows:

- The Real-time metrics page refreshes every 15 seconds, as long as the page is active. For example, if you have multiple tabs open in your browser and navigate to a different tab, the real-time metric page won't be updated until you return to it.
- Metrics such as Active and Availability refresh as activity occurs, with a small system delay for processing the activity.
- Agent near real-time metrics, such as Missed and Occupancy, refresh as activity occurs, with a small delay for processing.
- Contact near real-time metrics refresh about a minute after a contact ends.

**Use one-click drill-downs for Routing profiles and Queues tables**

In real-time metrics reports, for Routing profiles and Queues tables, you can open pre-filtered tables that display the associated queues, routing profiles, or agents. These one-click filters provide a way for you to drill into the performance data.
Example 1: Queues table -> Routing profiles table -> Agents table

For example, at a Queues table, choose the dropdown and then choose View routing profiles, as shown in the following image.

Below the Queues table, a Routing profiles table appears, as shown in the following image. It is filtered to display only the routing profiles associated with the queue. On the Routing profiles table, you can choose quick filters to display queues or agents only associated with that routing profile.
Example 2: Queues table -> Agents table

At the Queues table, choose View agents. Below the Queues table, an Agents table appears. It is filtered to display all the agents working that queue, as shown in the following image. The agents may be associated with different routing profiles.
Visualize: Queue dashboard

You can visualize historical queue data using time series graphs to help identify patterns, trends, and outliers such as Service Level, Contacts Queued, and Average Handle Time.

To view queue data

1. On the **Real-time Metrics** page, display the Queues table.
2. Select **View queue graphs** from the dropdown menu. The following image shows the dropdown menu for a queue named **test queue**.
3. After you select **View queue graphs**, you are directed to the queue visualization dashboard.

4. The Queue dashboard automatically refreshes every 15 minutes. You can:
   
   - Configure a time range of up to 24 hours.
   - Select the channel of your choice.
   - Customize the service level thresholds.

The following image shows an example Queue dashboard. It displays a graph of service level data for the queue. **Time range** is set to **Previous 24 hours to future 24 hours**. **Channel** is set to **All channels**. **Service level** is set to **60 seconds**.
View how many contacts are waiting in queue

To see the number of customers waiting in queue

1. Go to **Analytics and optimization, Real-time metrics, Queues**.
2. On the **Real-time metrics** page, **Queues** table, view the data in the **In queue** column.

*In queue* shows the count of all customers who are in waiting a queue for an agent, including the callback customers.

View contacts in queue

1255

View how many contacts are in an agent's queue

To see how many contacts are in an agent's personal queue, add an **Agent queues** table to your **Real-time metrics, Queues** report. Then view these two metrics:

- **In Queue**—how many contacts are in an agent's personal queue.
- **Queued**—the number of contacts added to their personal queue during the specified time range.

Use the following procedure.

1. Go to **Analytics and optimization, Real-time metrics, Queues**.
2. Choose **New table, Agent queues** as shown in the following image.
The **In queue** column displays how many contacts are in the agent's queue.

3. Review the metrics in the **In queue** and **Queue** columns.

**Tip**

An agent is included in the **Agent queues** table only if they are online or there is at least one contact in their queue.

**Add In Queue and Queue to the Agent queue table**

If **In queue** or **Queue** don't appear in your **Agent queue** table, use the following steps to add them.

1. On the **Agent queues** table, choose **Settings**, as shown in the following image.
2. Choose the **Metrics** tab.

3. Scroll to the **Performance** section and choose **In queue** and **Queued**, and then **Apply**, as shown in the following table.

```
<table>
<thead>
<tr>
<th>Queued</th>
<th>Handled</th>
<th>Abandoned</th>
<th>AHT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The changes appear in your table immediately.

4. Choose **Save** to add this report to your list of Saved reports.
View how many contacts are waiting for a callback

To see only the number of customers who are waiting for a call back, you need to create a queue that only takes callback contacts. To learn how to do this, see Set up routing.

Currently there isn't a way to see the phone numbers of the contacts waiting for callbacks.

Create a real-time metrics report

You can create a real-time metrics report to view real-time or near-real time metrics data for activity in your contact center. You must have permission to access metric data. The CallCenterManager and QualityAnalyst security profiles include this permission. For more information, see Security profiles.

To create a real-time metrics report

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Choose Analytics and optimization, Real-time metrics.
3. Choose one of the following report types. They group and order the data in different ways and include different metrics by default.
   - Queues
   - Agents
   - Routing profiles
4. To add another report to the page, choose New table and then choose a report type. You can add multiple reports of the same report type.
   
   There's no limit to the number of tables you can add, but you might start experiencing performance issues if you add a lot of them.
5. To customize a report, choose the gear icon from its table.
6. On the Time Range tab, do the following:
   
   a. For Trailing windows for time, select the time range, in hours, for the data to include in the report.
   b. (Optional) If you select Midnight to now, the time range is from midnight to the current time, based on the Time Zone that you select. If you select a time zone other than the one you are currently in, the time range starts at midnight for the calendar day in that time zone, not your current time zone.
7. (Optional) On the Filters tab, specify filters to scope the data to be included in the report. The available filters depend on the report type. The following are the possible filters:

- **Agents**—Includes data only for the agents that you select from **Include**.
- **Agent Hierarchies**—Includes data only for the agent hierarchies that you select from **Include**.
- **Queues**—Includes data only for the queues that you select from **Include**.
- **Routing profiles**—Includes data only for the routing profiles that you select from **Include**.

8. On the Metrics tab, choose the metrics and fields to include in the report. The available metrics and fields depend on the report type and filters that you select. For more information, see [Real-time metrics definitions](#).

9. When you are finished customizing the report, choose **Apply**.

10. (Optional) To save your report for future reference, choose **Save**, provide a name for the report, and then choose **Save**.

    To view your saved real-time metrics reports, choose **Analytics and optimization**, **Saved reports**, and then choose the **Real-time metrics** tab.

### No metrics or too few rows in a queues report?

It's possible to run a manually configured queues report and have no metrics returned, or fewer rows than expected.

This is because a queues report only includes data for a maximum of 100 queues, using one row per queue. If a queue doesn't have any activity* during the time range for the report, it's excluded from the report rather than included with null values. This means that if you create a report, and there is no activity for any of the queues included in the report, your report will not include any data.

This applies to the `GetCurrentMetricsData` API as well. This means that if a queue is not considered active, if you query for its metrics using the API you won't get any data.

**Tip**

*Here's how we define whether a queue is active: there's at least one contact in queue or there's at least one online agent for that queue. Otherwise, it's considered inactive.*
Real-time metrics reports do not include agents who have been inactive for approximately the past 5 minutes. For example, after the agent changes their CCP status to **Offline**, their username continues to appear in the Real-time metrics report for another approximately 5 minutes. At the 5 minute point, the agent no longer appears in the report.

In the following situations, you could end up with no metrics or fewer rows than expected:

1. You're attempting to run a report with no filters or groupings, and have more than 100 queues in your instance. The report pulls metrics for the first 100 queues, and then displays only those that are active.

2. You're attempting to run a report with filters and groupings, but it still has more than 100 queues matching that criteria. To process this request, Amazon Connect applies all the specified filters and groupings. This pulls the first 100 queues matching that criteria. Then out of those queues, it displays only the active ones.

   For example, let's say you have 300 queues in your instance. Of these, 200 match your criteria; 100 are active and by coincidence all happen to be Queues #100-#200. When you run the report, you'd get just 1 row (Queue #100) since the other 99 queues that were returned (Queues #1-#99) were considered inactive and were not displayed.

3. You're running a report with fewer than 100 queues. While you may expect to see metrics for all filtered queues, only active queues are shown on the real-time metrics report page. Try changing the settings for the report, such as changing the time range.

**List queues grouped by routing profile**

1. Go to **Analytics and optimization**, **Real-time metrics**, **Queues**.
2. Click **Settings**.
3. On the **Groupings** tab, choose **Queues grouped by routing profiles**.

4. Choose **Apply**.

**List agents grouped by routing profile**

1. Go to Analytics and optimization, Real-time metrics, Queues.

2. Choose **New table, Agents**.

3. Click **Settings**, as shown in the following image.

![Real-time metrics](image)

4. On the **Filters** tab, choose **Routing profiles** from the **Filter primary groupings by** dropdown list. In **Include**, select the routing profiles you want included in the table, as shown in the following image.

![Table Settings](image)

5. Choose **Apply**.
Sort agents by activity in a real-time metrics report

On the real-time metrics **Agents** report, you can sort agents by **Activity** when agents are enabled to use the same channel.

For example, the following image shows that you can sort agents by the **Activity** column because all the agents are enabled to use the same channel: voice.

![Image of agents sorted by activity](image)

However, if one or more agents are enabled to handle voice, chat, and tasks—or any two of the channels—you can't sort them by the **Activity** column because of the multiple channels. In this case, there's no option to sort by the **Activity** column, as shown in the following image:

![Image of agents with multiple channels](image)

**Note**

The real-time metrics Agents report doesn't support secondary sorting. For example, you can't sort by **Activity**, and then sort by **Duration**.
Change the "Agent activity" status in a real-time metrics report

Agents manually set their status in the Contact Control Panel (CCP). However, on the real-time metrics report, managers can manually change the Agent Activity status of an agent. This overrides what the agent has set in the CCP.

The value that's displayed in the Agent Activity column can be either:

- The agent's availability status, such as Offline, Available, or Break.
- The contact state, such as Incoming or On contact.

When you choose the Agent Activity column, you can select and change an agent's availability status, such as Offline, Available, or Break. The following image shows an example where only the Available status is in the dropdown list of the Activity column.

![Agent Activity column example](image)

This change appears in the agent event stream.

However, when a contact state is displayed in the Agent Activity column, such as Incoming or On contact, you cannot change it to Available or Offline, for example, even though those options are displayed in the dropdown menu, as shown in the following image. This means you can't set the agent's next status while they are on a contact.

![Agent Activity column contact state example](image)
You'll get an error message that says *Error changing agent status*, as shown in the following image.

**Required permissions to change an agent's activity status**

For someone such as a manager to be able to change an agent's activity status, they need to be assigned a security profile that has the following permissions:

- View - Agent Status
- Access metrics

The **Agent status - View** permission is shown in the following image of the Users and permissions section of the security profile page.

The **Access metrics - Access** permission is shown in the following image of the Analytics and Optimization section of the security profile page.
You can download the data included in your report as a comma-separated value (CSV) file so that you can use it with other applications. If there is no data for one of the selected metrics, the field in the downloaded CSV file contains a dash.

All exported times are in seconds.

**To download a real-time metrics report as a CSV file**

1. Create the report.
2. Choose the down arrow next to **Save** in the top-right corner of the page and choose **Download CSV**.
3. When prompted, confirm whether to open or save the file.

The following image shows real-time metrics in a Queue table. All times in the online report are in hours:minutes:seconds (hh:mm:ss). Below the image of the Queue table, there is an image of the same data in a downloaded CSV file opened with Excel. All times in the downloaded report are in seconds.
You can convert the seconds to minutes using an Excel formula. Alternatively, if you have a short report, you can copy and paste the data from Amazon Connect to Excel and it will preserve the format.

**Historical metrics reports**

Historical metrics reports include data about past, completed activity and performance in your contact center. Amazon Connect includes built-in historical reports that you can start using right away. You can also build your own custom reports.

When creating and analyzing your historical metrics reports, keep in mind that there are two categories of metrics:

**Contact record-driven metrics**

These metrics are based on formed contact record records. For a given interval, contact records whose disconnect date falls in the interval are selected to calculate metrics. For example, if a contact starts at 05:23 and ends at 06:15, this contact contributes 52 minutes of metrics for the 06:00-06:30 interval.
Example contact record-driven metrics are **Service level**, **Agent interaction time**, and **After contact work time**.

**Agent activity-driven metrics**

These metrics are based on agent activities, like agent status changes, agent conversation changes. The metrics reflect on the actual time the activity happens. For example, if agent handles a contact from 05:23 to 06:15, the **Agent on contact time** has 7 minutes for the 05:00-05:30 interval, 30 minutes for the 05:30-06:00 interval, and 15 minutes for the 06:00-06:30 interval.

For example, an agent activity-driven metric is **Non-Productive Time**.

You can customize the report settings to get the view of the data that is most meaningful for your organization. You can change the time frame for the report, which metrics are included in the report, and how data is grouped in the report. After you have customized a report, you can save it for future reference. You can generate a report using a recurring schedule that you define.

**Contents**

- [Historical metrics definitions](#)
- [Permissions required to view historical metrics reports](#)
- [Tag-based access control for historical metrics reports](#)
- [Create a historical metrics report](#)
- [Historical report limits](#)
- [Schedule a historical metrics report](#)
- [Update a historical metrics report](#)
- [Download a historical metrics report](#)
- [Show agent queues in a Queues table](#)
- [How many contacts in queue on a specific date](#)
- [Agent activity audit report](#)

**Historical metrics definitions**

The following metrics are available to include in historical metrics reports in Amazon Connect unless otherwise noted.
Developers can use the `GetMetricDataV2` and `GetMetricData` APIs to get a subset of the following historical metrics from the specified Amazon Connect instance.

### Tip

We recommend using the `GetMetricDataV2` API. It provides more flexibility, features, and the ability to query longer time ranges than `GetMetricData`. Use it to retrieve historical agent and contact metrics for the last 3 months, at varying intervals. You can also use it to build custom dashboards to measure historical queue and agent performance. For example, you can track the number of incoming contacts for the last 7 days, with data split by day, to see how contact volume changed per day of the week.

---

**Abandonment rate**

This metric is available only by using the `GetMetricDataV2` API; it is not available in the Amazon Connect admin website.

The percentage of contacts that were disconnected by the customer while in the queue. Contacts queued for callback are not counted as abandoned.

In the `GetMetricDataV2` API, this metric can be retrieved by using `ABANDONMENT_RATE`.

**Type:** String (`hh:mm:ss`)

**Min value:** 0.00%

**Max value:** 100.00%

**Category:** contact record-driven metric

**Adherence**

This metric is available only in AWS Regions where Forecasting, capacity planning, and scheduling is available.

The percentage of time that an agent correctly follows their schedule. This is measured by tracking if an agent is in an `Available` agent status when they should be in productive state. This percentage is calculated as follows:

\[
\text{Adherence} \% = \left( \frac{\text{Total Adherent Minutes}}{\text{Total Scheduled Adherence Minutes}} \right)
\]
An agent is considered adherent if the agent is in an *Available* status, when the shift activity is *Productive*, or if the agent is in *Non-Productive* status (for example, a custom status), when the shift activity is Non-Productive. Otherwise the agent is considered non-adherent. This means that if a shift activity is named *Lunch* but marked as productive, the agent is considered adherent if they are in the *Available* agent status.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `AGENT_SCHEDULE_ADHERENCE`.

Type: String

Min value: 0.00%

Max value: 100.00%

Category: Agent activity-driven metric

**Note**

Any time you change the schedule, Schedule Adherence is re-calculated up to 30 days in the past from the current date (not the date of the schedule), if schedules are changed.

### Adherent time

This metric is available only in AWS Regions where [Forecasting, capacity planning, and scheduling](#) is available.

The total time an agent was in an *Available* status when their shift activity is productive or was in non-productive status when the shift activity is non-productive.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `AGENT_ADHERENT_TIME`.

Type: String

Category: Agent activity-driven metric

### After contact work time

The total time that an agent spent doing ACW for a contact. In some businesses, also known as Call Wrap Up time.
You specify the amount of time an agent has to do ACW in their agent configuration settings. When a conversation with a contact ends, the agent is automatically allocated to do ACW for the contact. They stop doing ACW for a contact when they indicate they are ready for another contact in the CCP.

In the GetMetricData API, this metric can be retrieved by using AFTER_CONTACT_WORK_TIME.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_AFTER_CONTACT_WORK_TIME.

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Agent answer rate**

Percentage of contacts routed to an agent that were answered.

In the GetMetricDataV2 API, this metric can be retrieved by using AGENT_ANSWER_RATE.

Type: String

Min value: 0.00%

Max value: 100.00%

Category: Agent activity-driven metric

**Agent API connecting time**

The total time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONNECTING_TIME_AGENT with a MetricFilters parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = API

Type: String (hh:mm:ss)

Category: Agent activity-driven metric
Agent callback connecting time

The total time between when a callback contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONNECTING_TIME_AGENT with a MetricFilters parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = API

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Agent first name

The first name of the agent, as entered in their Amazon Connect user account. This metric is available only when grouping by agent.

Type: String

Length: 1-255

Agent idle time

After the agent sets their status in the CCP to Available, this is the amount of time they weren't handling contacts + any time their contacts were in an Error state.

Agent idle time doesn't include the amount of time from when Amazon Connect starts routing the contact to the agent, to when agent picks up or declines the contact.

Note

This metric can't be grouped or filtered by queue. For example, when you create a historical metrics report and filter by one or more queues, Agent idle time is not displayed.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_IDLE_TIME_AGENT.

Type: String (hh:mm:ss)
Agent incoming connecting time

The total time between when a contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the agent event stream, this is the duration between the contact state of STATE_CHANGE event changes from CONNECTING to CONNECTED/MISSED/ERROR.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_CONNECTING_TIME_AGENT` with a `MetricFilters` parameter set as follows:

- `MetricFilterKey = INITIATION_METHOD`
- `MetricFilterValues = API`

Type: String (hh:mm:ss)

Agent interaction and hold time

Sum of Agent interaction time and Customer hold time.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_INTERACTION_AND_HOLD_TIME`.

Type: String (hh:mm:ss)

Agent interaction time

Total time that agents spent interacting with customers on inbound and outbound contacts. This does not include Customer Hold Time or After Contact Work Time.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_INTERACTION_TIME`.

Type: String (hh:mm:ss)
Agent last name

The last name of the agent, as entered in their Amazon Connect user account. This metric is available only when grouping by agent.

Type: String
Length: 1-255

Agent name

The name of the agent, displayed as follows: Agent last name, Agent first name. This metric is available only when grouping by agent.

Agent non-response

The count of contacts routed to an agent but not answered by that agent, including contacts abandoned by the customer.

If a contact is not answered by a given agent, we attempt to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times (including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

This metric appears as Contacts missed in scheduled reports and exported CSV files.

In the GetMetricData API, this metric can be retrieved by using CONTACTS_MISSED.

In the GetMetricDataV2 API, this metric can be retrieved by using AGENT_NON_RESPONSE.

Type: Integer
Category: Agent activity-driven metric

Agent non-response without customer abandons

This metric is available only by using the GetMetricDataV2 API; it is not available in the Amazon Connect admin website.

The count of contacts routed to an agent but not answered by that agent, excluding contacts abandoned by the customer.

If a contact is not answered by a given agent, Amazon Connect attempts to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times...
(including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

In the GetMetricDataV2 API, this metric can be retrieved by using AGENT_NON_RESPONSE_WITHOUT_CUSTOMER_ABANDONS.

Data for this metric is available starting from October 1, 2023 0:00:00 GMT.

Type: Integer

Category: Agent activity-driven metric

**Agent on contact time**

Total time that an agent spent on a contact, including **Customer Hold Time** and **After Contact Work Time**. This does **not** include time spent on a contact while in a custom status or **Offline** status. (Custom status = the agent's CCP status is other than **Available** or **Offline**. For example, Training would be a custom status.)

*Tip*

If you want to include the time spent in a custom status and **Offline** status, see **Contact handle time**.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONTACT_TIME_AGENT.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

**Agent outbound connecting time**

Total time between when an outbound contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONNECTING_TIME_AGENT with a **MetricFilters** parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = API
Type: String (hh:mm:ss)  
Category: Agent activity-driven metric

**API contacts**

The count of contacts that were initiated using an Amazon Connect API operation, such as StartOutboundVoiceContact. This includes contacts that were not handled by an agent.

Type: Integer  
Category: contact record-driven metric

**API contacts handled**

The count of contacts that were initiated using an Amazon Connect API operation, such as StartOutboundVoiceContact, and handled by an agent.

In the [GetMetricData](#) API, this metric can be retrieved by using API_CONTACTS_HANDLED.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using CONTACTS_HANDLED with a MetricFilters parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = API

Type: Integer  
Category: contact record-driven metric

**Average after contact work time**

Average amount of time that an agent spent doing After Contact Work (ACW) for contacts. This is calculated by averaging AfterContactWorkDuration (from the contact record) for all contacts included in the report, based on the selected filters.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using AVG_AFTER_CONTACT_WORK_TIME.

Type: String (hh:mm:ss)  
Category: contact record-driven metric
**Average agent API connecting time**

The average time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/api/v2-reference.html) API, this metric can be retrieved by using `AVG_AGENT_CONNECTING_TIME` with a `MetricFilters` parameter set as follows:

- `MetricFilterKey = INITIATION_METHOD`
- `MetricFilterValues = API`

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

**Average agent callback connecting time**

The average time between when a callback contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/api/v2-reference.html) API, this metric can be retrieved by using `AVG_AGENT_CONNECTING_TIME` with a `MetricFilters` parameter set as follows:

- `MetricFilterKey = INITIATION_METHOD`
- `MetricFilterValues = CALLBACK`

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

**Average agent incoming connecting time**

The average time between when contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected. This is the ring time for configurations where the agent is not set to auto-answer.

No equivalent to this metric is available in the GetMetricData API.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/api/v2-reference.html) API, this metric can be retrieved by using `AVG_AGENT_CONNECTING_TIME` with a `MetricFilters` parameter set as follows:
• MetricFilterKey = INITIATION_METHOD
• MetricFilterValues = INBOUND

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

**Average agent interaction and customer hold time**

Average of the sum of the agent interaction and customer hold time. This is calculated by averaging the sum of the following values from the contact record: AgentInteractionDuration and CustomerHoldDuration.

In the GetMetricData API, this metric can be retrieved by using INTERACTION_AND_HOLD_TIME.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_INTERACTION_AND_HOLD_TIME.

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Average agent interaction time**

Average time that agents interacted with customers during inbound and outbound contacts. This does not include Customer Hold Time or After Contact Work Time.

In the GetMetricData API, this metric can be retrieved by using INTERACTION_TIME.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_INTERACTION_TIME.

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Average agent outbound connecting time**

The average time between when an outbound contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_AGENT_CONNECTING_TIME with a MetricFilters parameter set as follows:
• MetricFilterKey = INITIATION_METHOD
• MetricFilterValues = OUTBOUND

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

**Average contact duration**

The average duration of a contact is calculated by taking the difference between their initiation time and their disconnect time (from the contact record) and dividing it by the total number of contacts. This metric reflects the average amount of time a contact spends from the moment they initiate the interaction to when they disconnect.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_CONTACT_DURATION.

![Note]
This metric is only available in the GetMetricDataV2 API.

Type: String (hh:mm:ss)

Category: Contact record-driven metric

**Average conversation duration**

The average conversation duration of voice contacts with agents is determined by calculating the total time from the start of the conversation until the last word spoken by either the agent or the customer. This value is then divided by the total number of contacts to provide an average representation of the conversation time spent on the call.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_CONVERSATION_DURATION.

![Note]
This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.
Type: String (hh:mm:ss)

Category: Contact Lens driven metric

**Average customer hold time**

Average time that customers spent on hold while connected to an agent. This is calculated by averaging `CustomerHoldDuration` (from the contact record).

In the [GetMetricData](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_GetMetricData.html) API, this metric can be retrieved by using `HOLD_TIME`.

In the [GetMetricDataV2](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_GetMetricData.html) API, this metric can be retrieved by using `AVG_HOLD_TIME`.

This average only includes contacts that went on hold.

Type: String (hh:mm:ss)

Category: contact record-driven metric

This metric doesn't apply to tasks so you'll notice a value of 0 on the report for them.

**Average customer hold time all contacts**

This metric is available only by using the [GetMetricDataV2](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_GetMetricData.html) API; it is not available in the Amazon Connect admin website.

Average hold time for all contacts handled by an agent. The calculation includes contacts that were never put on hold.

In the [GetMetricDataV2](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_GetMetricData.html) API, this metric can be retrieved by using `AVG_HOLD_TIME_ALLCONTACTS`.

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Average greeting time agent**

This metric represents the average first response time of agents on chat, indicating how quickly they engage with customers after joining the chat. It is calculated by dividing the total time it takes for an agent to initiate their first response by the number of chat contacts.

In the [GetMetricDataV2](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_GetMetricData.html) API, this metric can be retrieved by using `AVG_GREETING_TIME_AGENT`. 

Historical metrics definitions
Note
This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

Type: String (hh:mm:ss)
Category: Contact Lens driven metric

Average handle time

The average time, from start to finish, that a contact was connected with an agent (average handled time). It includes talk time, hold time, and After Contact Work (ACW) time.

AHT is calculated by averaging the amount of time between the contact being answered by an agent and the conversation ending. It applies to both inbound and outbound calls.

AHT is different from Contact handle time. AHT does not include any time spent in a custom status; Contact handle time (CHT) does include it.

In the GetMetricData API, this metric can be retrieved by using HANDLE_TIME.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_HANDLE_TIME.

Type: String (hh:mm:ss)
Category: contact record-driven metric

Average holds

This metric determines the average number of times a voice contact was put on hold while interacting with an agent. It is calculated by dividing the total number of holds by the total number of contacts, providing an average representation of the number of holds experienced per contact.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_HOLDS.

Note
This metric is only available in the GetMetricDataV2 API.
Type: String (hh:mm:ss)
Category: contact record-driven metric

**Average interruptions agent**

This metric quantifies the average frequency of agent interruptions during customer interactions by dividing the total number of agent interruptions by the total number of contacts.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using AVG_INTERRUPTIONS_AGENT.

<i>Note</i>

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the [GetMetricDataV2](#) API.

Type: String (hh:mm:ss)
Category: Contact Lens driven metric

**Average interruption time agent**

Average of total agent interruption time while talking to a contact. Calculating the average duration of agent interruptions during contact conversations involves summing the interruption intervals within each conversation and dividing the total by the number of conversations that experienced at least one interruption.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using AVG INTERRUPTION TIME AGENT.

<i>Note</i>

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the [GetMetricDataV2](#) API.
Average non-talk time

Average of total non-talk time in a voice conversation. Non-talk time refers to the combined duration of hold time and periods of silence exceeding 3 seconds, during which neither the agent nor the customer is engaged in conversation. To calculate non-talk time, we add up all the intervals in which both participants remained silent and then divide this total by the number of contacts.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_NON_TALK_TIME.

Note

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

Type: String (hh:mm:ss)

Category: Contact Lens driven metric

Average outbound after contact work time

Average time that agents spent doing After Contact Work (ACW) for an outbound contact.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_AFTER_CONTACT_WORK_TIME with a MetricFilters parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = OUTBOUND

Type: String (hh:mm:ss)

Category: contact record-driven metric

Average outbound agent interaction time

Average time that agents spent interacting with a customer during an outbound contact.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_INTERACTION_TIME with a MetricFilters parameter set as follows:
• MetricFilterKey = INITIATION_METHOD
• MetricFilterValues = OUTBOUND

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Average queue abandon time**

Average time that contacts waited in the queue before being abandoned. This is calculated by averaging the difference between `EnqueueTimestamp` and `DequeueTimestamp` (from the contact record) for abandoned contacts.

A contact is considered abandoned if it was removed from a queue but not answered by an agent or queued for callback.

In the [GetMetricData](https://docs.aws.amazon.com/connect/latest/customerguide/gdm.html) API, this metric can be retrieved by using ABANDON_TIME.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/customerguide/gmvd.html) API, this metric can be retrieved by using AVG_ABANDON_TIME.

Type: String (hh:mm:ss)

Category: contact record-driven metric

**Average queue answer time**

Average time that contacts waited in the queue before being answered by an agent. In some businesses, this is also known as average speed of answer (ASA).

Average queue answer time also includes the time during the agent whisper, because the contact remains in queue until the agent whisper is completed.

This is the average of Duration (from the contact record).

In the [GetMetricData](https://docs.aws.amazon.com/connect/latest/customerguide/gdm.html) API, this metric can be retrieved by using QUEUE_ANSWER_TIME.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/customerguide/gmvd.html) API, this metric can be retrieved by using AVG_QUEUE_ANSWER_TIME.

Type: String (hh:mm:ss)

---

### Historical metrics definitions

1283
**Category: contact record-driven metric**

**Average resolution time**

This metric is available only by using the [GetMetricDataV2](#) API; it is not available in the Amazon Connect admin website.

The average time, beginning from the time a contact was initiated to the time it resolved. The resolution time for a contact is defined as: beginning from `InitiationTimestamp`, and ending at `AfterContactWorkEndTimestamp` or `DisconnectTimestamp`, whichever one is later.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `AVG_RESOLUTION_TIME`.

Type: String (`hh:mm:ss`)

**Average talk time**

Average time that was spent talking during a voice contact across either the customer or the agent. This is calculated by summing up all the intervals in which either an agent, a customer, or both were engaged in conversation, and then dividing it by the total number of contacts.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `AVG_TALK_TIME`.

Type: String (`hh:mm:ss`)

**Average talk time agent**

Average time that was spent talking in a conversation by an agent. This is calculated by summing up the durations of all intervals during which the agent was speaking and then dividing that sum by the total number of contacts.

---

*Note*

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the [GetMetricDataV2](#) API.
In the GetMetricDataV2 API, this metric can be retrieved by using AVG_TALK_TIME_AGENT.

**Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

Type: String (hh:mm:ss)

Category: Contact Lens driven metric

**Average talk time customer**

Average time that was spent talking in a conversation by a customer. This is calculated by summing up the durations of all intervals during which the customer was speaking and then dividing that sum by the total number of contacts.

In the GetMetricDataV2 API, this metric can be retrieved by using AVG_TALK_TIME_CUSTOMER.

**Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

Type: String (hh:mm:ss)

Category: Contact Lens driven metric

**Callback attempts**

The number of contacts where a callback was attempted, but the customer did not pick up.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_RETRY_CALLBACK_ATTEMPTS.

Type: Integer

Category: contact record-driven metric
Callback contacts

The count of contacts that were initiated from a queued callback.

- Type: Integer
- Category: contact record-driven metric

Callback contacts handled

The count of contacts that were initiated from a queued callback and handled by an agent.

In the `GetMetricData` API, this metric can be retrieved by using `CALLBACK_CONTACTS_HANDLED`.

In the `GetMetricDataV2` API, this metric can be retrieved by using `CONTACTS_HANDLED` with a `MetricFilters` parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = CALLBACK

Type: Integer

Category: contact record-driven metric

Contact disconnected

Sum of contacts disconnected in a queue. The metric can be filtered by Disconnect Reason.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_CONTACTS_DISCONNECTED`.

- Type: Integer
- Category: contact record-driven metric

Contact flow time

Total time a contact spent in a flow.

Outbound contacts don't start in a flow, so outbound contacts aren't included.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_CONTACT_FLOW_TIME`.

Historical metrics definitions
• Type: String \( hh:mm:ss \)
• Category: contact record-driven metric

**Contact abandoned**

The count of contacts disconnected by the customer while in the queue. Contacts queued for callback are not counted as abandoned. When you create customized historical reports, to include this metric, on the **Groupings** tab choose either **Queue** or **Phone Number**.

In the [GetMetricData](#) and [GetMetricDataV2](#) APIs, this metric can be retrieved by using CONTACTS_ABANDONED.

• Type: Integer
• Category: contact record-driven metric

**Contact handle time**

Total time that an agent spent on contacts, including **Customer Hold Time** and **After contact work time**. This includes any time spent on contacts while in a custom status. (Custom status = the agent's CCP status is other than **Available** or **Offline**. For example, Training would be a custom status.)

**Tip**

If you want to exclude the amount of time spent in a custom status, see [Agent on contact time](#).

In the [GetMetricDataV2](#) API, this metric can be retrieved by using **SUM_HANDLE_TIME**
Contacts abandoned in $X$ seconds

The count of contacts disconnected by the customer while in the queue for 0 to $X$ seconds. The possible values for $X$ are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONTACTS_ABANDONED_IN_X. The API enables you to create custom duration to get this metric. Choose from additional durations, such as minutes, hours, or days. The maximum duration for a custom value is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

Contacts agent hung up first

The count of contacts disconnected where the agent disconnected before the customer.

In the GetMetricData API, this metric can be retrieved by using CONTACTS_AGENT_HUNG_UP_FIRST.

In the GetMetricDataV2 API, this metric can be retrieved by using CONTACTS_HANDLED with a MetricFilters parameter set as follows:

- MetricFilterKey = DISCONNECT_REASON
- MetricFilterValues = AGENT_DISCONNECT

Contacts answered in $X$ seconds

The count of contacts that were answered by an agent between 0 and $X$ seconds of being placed in the queue, based on the value of EnqueueTimestamp. The possible values for $X$ are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.
In the GetMetricDataV2 API, this metric can be retrieved by using SUM_CONTACTS_ANSWERED_IN_X. The API enables you to create custom duration to get this metric. Choose from additional durations, such as minutes, hours, or days. The maximum duration for a custom value is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

- Type: Integer
- Category: contact record-driven metric

**Contacts created**

The count of contacts in a queue. The metric can be filtered by initiation methods.

In the GetMetricDataV2 API, this metric can be retrieved by using CONTACTS_CREATED.

- Type: Integer
- Category: contact record-driven metric

**Contacts consulted**

Deprecated May 2019. When used in a report, it returns a dash (-).

The count of contacts handled by an agent who consulted with another agent in Amazon Connect. The agent interacts with the other agent, but the customer is not transferred to the other agent.

In the GetMetricData API, this metric can be retrieved by using CONTACTS_CONSULTED.

- Type: Integer
- Category: contact record-driven metric

**Contacts handled**

The count of contacts that were connected to an agent.

It doesn't matter how the contact got to the agent. It could be a customer calling your contact center, or an agent calling the customer. It could be a contact transferred from one agent to another. It could be a contact where the agent answered it, but then they weren't sure what to do...
and they transferred the contact away again. As long as the agent was connected to the contact, it increments **Contacts handled**.

In the [GetMetricData](#) and [GetMetricDataV2](#) APIs, this metric can be retrieved by using CONTACTS_HANDLED.

Type: Integer

Category: contact record-driven metric

**Contacts handled incoming**

The count of incoming contacts that were handled by an agent, including inbound contacts and transferred contacts. This includes contacts for all channels, such as voice, chat, tasks.

In the [GetMetricData](#) API, this metric can be retrieved by using CONTACTS_HANDLED_INCOMING.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using CONTACTS_HANDLED with a **MetricFilters** parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = INBOUND, TRANSFER, QUEUE_TRANSFER

Type: Integer

Category: contact record-driven metric

**Contacts handled outbound**

The count of outbound contacts that were handled by an agent. This includes contacts that were initiated by an agent using the CCP.

In the [GetMetricData](#) API, this metric can be retrieved by using CONTACTS_HANDLED_OUTBOUND.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using CONTACTS_HANDLED with a **MetricFilters** parameter set as follows:

- MetricFilterKey = INITIATION_METHOD
- MetricFilterValues = OUTBOUND

Type: Integer
Category: contact record-driven metric

**Contacts hold agent disconnect**

The count of contacts that were disconnected by the agent while the customer was on hold.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/admguides/api-get-metric-data-v2.html) API, this metric can be retrieved by using `CONTACTS_ON_HOLD_AGENT_DISCONNECT`.

- Type: Integer
- Category: contact record-driven metric

**Contacts hold customer disconnect**

The count of contacts that were disconnected by the customer while the customer was on hold.

In the [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/admguides/api-get-metric-data-v2.html) API, this metric can be retrieved by using `CONTACTS_ON_HOLD_CUSTOMER_DISCONNECT`.

- Type: Integer
- Category: contact record-driven metric

**Contacts hold disconnect**

The count of contacts disconnected while the customer was on hold. This includes both contacts disconnected by the agent and contacts disconnected by the customer.

In the [GetMetricData](https://docs.aws.amazon.com/connect/latest/admguides/api-get-metric-data.html) and [GetMetricDataV2](https://docs.aws.amazon.com/connect/latest/admguides/api-get-metric-data-v2.html) APIs, this metric can be retrieved by using `CONTACTS_HOLD_ABANDONS`.

- Type: Integer
- Category: contact record-driven metric

**Contacts incoming**

The count of incoming contacts, including inbound contacts and transferred contacts.

- Type: Integer
• Category: contact record-driven metric

Contacts put on hold

The count of contacts put on hold by an agent one or more times.

In the GetMetricDataV2 API, this metric can be retrieved by using CONTACTS_PUT_ON_HOLD.

• Type: Integer
• Category: contact record-driven metric

Contacts queued

The count of contacts placed in the queue.

In the GetMetricData and GetMetricDataV2 APIs, this metric can be retrieved by using CONTACTS_QUEUED.

• Type: Integer
• Category: contact record-driven metric

Contacts resolved in X

This metric is available only by using the GetMetricDataV2 API; it is not available in the Amazon Connect admin website.

The count of contacts that have a resolution duration between 0 and X seconds after being initiated based on InitiationTimestamp. The resolution time for a contact is defined as: beginning from InitiationTimestamp, and ending at AfterContactWorkEndTimestamp or DisconnectTimestamp, whichever one is later.

The GetMetricDataV2 API enables you to create custom duration to get this metric. Choose from additional durations, such as minutes, hours, or days. The maximum duration for a custom value is 7 days. That's because in Amazon Connect you can't have a contact that lasts longer than 7 days.

In the GetMetricDataV2 API, this metric can be retrieved by using CONTACTS_RESOLVED_IN_X.

Type: Integer
Category: contact record-driven metric

**Contacts transferred in**

The count of contacts transferred in from queue to queue, and transferred in by an agent using the CCP.

In the [GetMetricData](#) API, this metric can be retrieved by using `CONTACTS_TRANSFERRED_IN`.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `CONTACTS_CREATED` with a [MetricFilters](#) parameter set as follows:

- **MetricFilterKey** = INITIATION_METHOD
- **MetricFilterValues** = TRANSFER, QUEUE_TRANSFER

Type: Integer

Category: contact record-driven metric

**Contacts transferred in by agent**

The count of contacts transferred in by an agent using the CCP.

In the [GetMetricData](#) API, this metric can be retrieved by using `CONTACTS_TRANSFERRED_IN_BY_AGENT`.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using `CONTACTS_CREATED` with a [MetricFilters](#) parameter set as follows:

- **MetricFilterKey** = INITIATION_METHOD
- **MetricFilterValues** = TRANSFER

Type: Integer

Category: contact record-driven metric

**Contacts transferred in from queue**

The count of contacts transferred to the queue from another in a **Transfer to queue** flow.

Historical metrics definitions
In the `GetMetricData` API, this metric can be retrieved by using `CONTACTS_TRANSFERRED_IN_FROM_Q`.

In the `GetMetricDataV2` API, this metric can be retrieved by using `CONTACTS CREATED` with a `MetricFilters` parameter set as follows:

- `MetricFilterKey = INITIATION_METHOD`
- `MetricFilterValues = QUEUE_TRANSFER`

Type: Integer

Category: contact record-driven metric

**Contacts transferred out**

The count of contacts transferred out from queue to queue, and transferred out by an agent using the CCP.

In the `GetMetricData` and `GetMetricDataV2` APIs, this metric can be retrieved by using `CONTACTS_TRANSFERRED_OUT`.

**Tip**

- **Contacts transferred out** includes all transferred contacts, including contacts who were not connected to an agent before they were transferred out.
- **Contacts transferred out by an agent** is limited to contacts who were connected to an agent before that agent transferred them out.

- Type: Integer
- Category: contact record-driven metric

**Contacts transferred out by agent**

The count of contacts transferred out by an agent using the CCP.

In the `GetMetricData` and `GetMetricDataV2` APIs, this metric can be retrieved by using `CONTACTS_TRANSFERRED_OUT_BY_AGENT`. 
Tip

- **Contacts transferred out** includes all transferred contacts, including contacts who were not connected to an agent before they were transferred out.
- **Contacts transferred out by an agent** is limited to contacts who were connected to an agent before that agent transferred them out.

- Type: Integer
- Category: contact record-driven metric

**Contacts transferred out external**

The count of contacts that an agent transferred from the queue to an external source, such as a phone number other than the phone number for your contact center.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using **CONTACTS_TRANSFERRED_OUT_EXTERNAL**.

- Type: Integer
- Category: contact record-driven metric

**Contacts transferred out internal**

The count of contacts for the queue that an agent transferred to an internal source, such as a queue or another agent. An internal source is any source that can be added as a quick connect.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using **CONTACTS_TRANSFERRED_OUT_INTERNAL**.

- Type: Integer
- Category: contact record-driven metric

**Contacts transferred out queue**

The count of contacts transferred from the queue to another queue in a **Transfer to queue** flow.
In the `GetMetricData` and `GetMetricDataV2` APIs, this metric can be retrieved by using `CONTACTS_TRANSFERRED_OUT_FROM_QUEUE`.

- Type: Integer
- Category: contact record-driven metric

**Customer hold time**

Total time that customers spent on hold after being connected to an agent. This includes time spent on a hold when being transferred, but does not include time spent in a queue.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_HOLD_TIME`.

- Type: String (`hh:mm:ss`)
- Category: contact record-driven metric

**Error status time**

For a specific agent, the total time contacts were in an error status. This metric can't be grouped or filtered by queue.

In the `GetMetricDataV2` API, this metric can be retrieved by using `SUM_ERROR_STATUS_TIME_AGENT`.

- Type: String (`hh:mm:ss`)
- Category: Agent activity-driven metric

**Maximum queued time**

The longest time that a contact spent waiting in the queue. This includes all contacts added to the queue, even if they were not connected with an agent, such as abandoned contacts.

In the `GetMetricData` API, this metric can be retrieved by using `QUEUED_TIME`.

In the `GetMetricDataV2` API, this metric can be retrieved by using `MAX_QUEUED_TIME`.

- Type: String (`hh:mm:ss`)
- Category: contact record-driven metric
Non-adherent time

This metric is available only in AWS Regions where Forecasting, capacity planning, and scheduling is available.

Total time an agent was not in an Available status when their shift activity is productive or not in a non-productive status when their shift activity is non-productive.

In the GetMetricDataV2 API, this metric can be retrieved by using AGENT_NON_ADHERENT_TIME.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric

Non-Productive Time

Total time that agents spent in a custom status. That is, their CCP status is other than Available or Offline.

This metric doesn't mean that the agent was spending their time unproductively.

Tip

Agents can handle contacts while their CCP status is set to a custom status. For example, agents can be On contact or doing ACW while their CCP is set to a custom status. This means it's possible for agents to be counted as On contact and NPT at the same time. For example, if an agent changes their status to a custom status, and then makes an outbound call, it would be counted as non-productive time.

When you create a historical metrics report, this metric can't be grouped or filtered by queue.

In the GetMetricDataV2 API, this metric can be retrieved by using SUM_NON_PRODUCTIVE_TIME_AGENT.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric
Non-talk time percent

The non-talk time in a voice conversation as a percent of the total conversation duration. To calculate non-talk time percent, Amazon Connect totals all the intervals in which participants remained silent (non-talk time), and then divides this total by the total conversation duration.

In the GetMetricDataV2 API, this metric can be retrieved by using PERCENT_NON_TALK_TIME.

**Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

- Type: Percent
- Category: Contact Lens driven metric

Occupancy

Percentage of time that agents were active on contacts. This percentage is calculated as follows:

\[
\frac{\text{Agent on contact (wall clock time)}}{\text{Agent on contact (wall clock time)} + \text{Agent idle time}}
\]

Where:

- (Agent on contact + Agent idle time) = total amount of agent time
- So \(\frac{\text{Agent on contact}}{\text{total amount of agent time}} = \text{percentage of time agents were active on contacts.}\)

**Important**

Occupancy doesn't account for concurrency. That is, an agent is considered 100% occupied for a given interval if they are handling at least one contact for that entire duration.

In the GetMetricData API, this metric can be retrieved by using OCCUPANCY.

In the GetMetricDataV2 API, this metric can be retrieved by using AGENT_OCCUPANCY.

- Type: String
• Min value: 0.00%
• Max value: 100.00%
• Category: Agent activity-driven metric

**Online time**

Total time that an agent spent with their CCP set to a status other than Offline. This includes any time spent in a custom status. When you create a historical metrics reports, this metric can't be grouped or filtered by queue, phone number, or channels.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using SUM_ONLINE_TIME_AGENT.

• Type: String
• Category: Agent activity-driven metric

**Scheduled time**

This metric is available only in AWS Regions where Forecasting, capacity planning, and scheduling is available.

Total time an agent was scheduled (either for productive or non-productive time) and Adherence for those shifts was set to Yes.

In the [GetMetricDataV2](#) API, this metric can be retrieved by using AGENT_SCHEDULED_TIME.

• Type: String ((hh:mm:ss)
• Category: Agent activity-driven metric

**Service level X**

Percentage of contacts removed from the queue between 0 and X after being added to it. A contact is removed from a queue when the following occurs: an agent answers the contact, the customer abandons the contact, or the customer requests a call back.

For X you can choose from pre-set times in seconds: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600. This percentage is calculated as follows:

\[
\text{(Contacts removed from queue in } X \text{ seconds / Contacts queued) } \times 100
\]
In the `GetMetricData` and `GetMetricDataV2` APIs, this metric can be retrieved by using `SERVICE_LEVEL`.

- Type: String
- Min value: 0.00%
- Max value: 100.00%
- Category: contact record-driven metric

**Custom service levels**

You can also create custom service level metrics. Choose from additional durations, such as minutes, hours, or days.

Custom service levels are localized to the report where they are created. For example, you create a report that has a custom service level of 75. You leave the page and then create another report. The custom service level 75 won't exist in the second report. You'll need to create it again.

The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

You can add up to 10 custom service levels per report.

**Talk time agent percent**

The talk time by an agent in a voice conversation as a percent of the total conversation duration. To calculate this metric, Amazon Connect totals all the intervals in which an agent was engaged in conversation (talk time agent), and then divides this total by the total conversation duration.

In the `GetMetricDataV2` API, this metric can be retrieved by using `PERCENT_TALK_TIME_AGENT`.

**Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the `GetMetricDataV2` API.

- Type: Percent
- Category: Contact Lens driven metric
**Talk time customer percent**

The talk time by a customer in a voice conversation as a percent of the total conversation duration. To calculate this metric, Amazon Connect totals all the intervals in which a customer was engaged in conversation, and then divides this total by the total conversation duration.

In the GetMetricDataV2 API, this metric can be retrieved by using PERCENT_TALK_TIME_CUSTOMER.

⚠️ **Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

- Type: Percent
- Category: Contact Lens driven metric

**Talk time percent**

The talk time in a voice conversation as a percent of the total conversation duration. To calculate talk time percent, Amazon Connect totals all the intervals in which either an agent, a customer, or both were engaged in conversation (talk time), and then divides this total by the total conversation duration.

In the GetMetricDataV2 API, this metric can be retrieved by using PERCENT_TALK_TIME.

⚠️ **Note**

This metric is available only for contacts analyzed by Contact Lens conversational analytics and is only available in the GetMetricDataV2 API.

- Type: Percent
- Category: Contact Lens driven metric
Permissions required to view historical metrics reports

To view historical metrics reports, you need to be assigned to a security profile that has either the **Access metrics - Access** permission or the **Real-time metrics - Access** permission. Note the following behavior when you assign these permissions:

- When **Access metrics - Access** is selected, the **Real-time metrics**, **Historical metrics**, and **Agent activity audit** permissions are also automatically assigned.
- When **Access metrics - Access** is assigned, you have access to all real-time and historical metrics reports.

The following image shows the **Analytics and Optimization** section of the **Security profile permissions** page. The **Access** option is selected for **Access metrics**, **Real-time metrics**, **Historical metrics**, and **Agent activity audit**.

If only **Historical metrics - Access** is selected, you have access to only historical metrics and no other analytics pages or reports. The following image shows the **Analytics and Optimization** section, with only **Historical metrics - Access** selected.
Tag-based access control for historical metrics reports

Amazon Connect does not currently support tag-based access controls for historical metrics reports.

Create a historical metrics report

Although Amazon Connect includes built-in historical reports, you can create your own custom reports so you look at only the data that's of interest to your organization.

Requirement

- You must have permission to access metric data. The following security profiles include this permission: CallCenterManager and QualityAnalyst. For more information, see Security profiles.

Grouping options

You can group the metrics included in your reports in different ways to provide greater insight into how your contact center is performing.

You can group reports by queue, agent, agent hierarchy, routing profile, or phone number. The metric calculations, and therefore metrics values displayed in the report, are different when reports are grouped differently. For example, if you group a report by queue, the value of a metric includes all contacts associated with the queue. If you group a report by agent, the values for the metrics associated with queues might not provide much insight.

When you create a report, the values for calculated metrics are displayed as rows in the report. The rows in the report are grouped by the grouping options you select. Grouping the data enables you to generate global data for your contact center, or more specific data for queues, agents, routing profiles, or agent hierarchy defined in your contact center.

For example, consider the Contacts handled metric. This metric is a count of the contacts handled during the time range defined for the report. Here are the results based on the grouping:

- **Queue** - The metric is the total number of contacts handled during the time range from that queue by all agents in your contact center.
- **Agent** - The metric is the total number of contacts handled by that agent during the time range across all queues and routing profiles.
• **Routing Profile** - The metric is the total number of contacts handled during the time range by agents assigned that routing profile.

• **Queue**, then **Agent**, then **Routing Profile** - The metric is the total number of contacts that agent assigned that routing profile handled from that queue.

Agent activity can be included in one routing profile at a time, but agents can switch between routing profiles over the reporting time interval. If agents are assigned multiple routing profiles and handle contacts from multiple queues, there are multiple rows in the report for each routing profile assigned to the agent and the queue that the agent handled contacts from.

**Filters**

When you customize a report, you can add filters to control which data is included in the report. You can filter on the following:

• **Queue**—Includes data only for the specified queues. If you don't specify any queues, all queues are included.

• **Routing profile**—Includes data only for the agents assigned to the specified routing profiles. If you don't specify any routing profiles, data for all agents for all routing profiles is included.

• **Agent hierarchy**—Includes data only for the contacts handled by agents in the specified hierarchies. If you don't specify a hierarchy, data for all contacts handled by agents in all hierarchies is included. When only one hierarchy is specified, you can specify a more granular filter within the hierarchy.

• **Phone number**—Includes data only for the contacts associated with the specified phone numbers. If you don't specify a phone number, data for all contacts associated with all phone numbers is included.

**How to create a historical metrics report**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Choose **Analytics and optimization, Historical metrics**.
3. Choose one of the following report types, which group and order the data in different ways, and include different metrics:

   • **Queues**
     • **Contact metrics**
4. To customize your report, choose the gear icon.

5. On the Interval & Time range tab, do the following:
   
a. For Interval, choose **30 minutes** to get a row for each 30-minute period in the time range, **Daily** to get a row for each day in the time range, or **Total** to get all data for the time range in a single row.

b. For Time Zone, select a time zone, which determines the hour at which a day starts. For example, to align the report with your calendar days, select the time zone for your location.

   You should use the same time zone for reports over time to get accurate and consistent metrics data for your contact center. Using different time zones for different reports may result in different data for the same time range selection.

c. The possible values for Time range depend on the value that you select for Interval. Alternatively, you can specify a custom time range.

   For Last x days and Month to date, the current day is not included in the report. Yesterday specifies the previous calendar day while Last 24 hours specifies the 24 hours prior to the current time.

6. (Optional) On the Groupings tab, choose up to five groupings. If you choose one grouping option, the data is grouped by that option. If you choose multiple grouping options, the data is grouped by the first grouping option and then by the subsequent grouping options. For more information, see Grouping options.

7. (Optional) On the Filters tab, specify filters to scope the data to be included in the report. The available filters depend on the groupings that you select. For more information, see Filters.

8. On the Metrics tab, choose the metrics and fields to include in the report. An exclamation point (!) is displayed next to any metrics that are not available based on the groupings that you selected. For more information, see Historical metrics definitions.

9. When you are finished customizing your report, choose Apply.
10. (Optional) To save your report for future use, choose **Save**, provide a name for the report, and then choose **Save**.

**Historical report limits**

Historical metrics reports have the following limits:

**Service quotas**

- Historical metrics reports have service quotas, such as **Reports per instance** and **Scheduled reports per instance**. When service quotas are breached, the following error message is displayed: *Report cannot be saved*. For more information about these quotas, see [Amazon Connect service quotas](#).

**Data only for active queues**

- You can get data only for active queues. A queue is inactive if there are no contacts in the queue and no agents available.

**Query data for three days at a time, for the past 2 days**

- When you create a report that uses 15 minute intervals, you can return data for three days at a time, for the past 35 days. For 30 minute intervals you can return data for only three days at a time, but the data is available based on the retention period of contact records.

**The availability of historical metric data is based on the retention period of contact records**

- Historical metrics are based contact records. For the current retention period for contact records, see [Amazon Connect feature specifications](#).

**For daily and total intervals**

- You can select up to 31 days in a single request.
80k cell limit

There is currently an 80k cell limitation on historical metrics reports and scheduled reports. This applies to the total number of cells (columns * rows), accounting for grouping and filtering.

For example, let's say you create a historical metrics report with this criteria:

- Grouped by agents
- With an interval of 30 minutes
- For the last 24 hours
- Configured to include only 5 metrics
- Filtered to show only contacts handled in BasicQueue

If only 10 agents handled contacts in BasicQueue during this time, then you would expect to see 
\[(24*2)*5*10 = 2400 \] cells that count towards the 80k limit.

A message informs you if you reach the limit.

Schedule a historical metrics report

Before you schedule a historical metrics report, here are a few things you need to know:

Others can access the report

- Scheduling a report makes the report accessible by any other users in your contact center who have permissions to view saved reports.

Anyone with Schedule permissions can create, edit, or delete the schedule of your report

- After you publish a report, any user with Saved reports - Schedule permissions in their security profile can create, edit, or delete the schedule of your report. They cannot delete the actual report.

Scheduled reports are located in an Amazon S3 bucket

- Scheduled reports are saved as CSV files in the Amazon S3 bucket specified for reports for your contact center. When you set up the scheduled report, you can add a prefix to the location in Amazon S3 for the report files.
• When the report is exported to your Amazon S3 bucket, the file name includes the date and UTC time when the report was created. The **Last modified date** for the file is displayed using the time zone for the Amazon S3 bucket, and may not match the creation time for the report, which is in UTC.

**There's a 15 minute delay**

• For scheduled reports, there is a delay of 15 minutes after the scheduled report time before the report is generated. This is to ensure that the report includes the data for all of the activity that occurred during the time range specified for the report. Data from your contact center is not immediately processed and available to include in reports, so some data from the time range might not be captured in a report if the report is generated at the second the time range ends.

• For example, if you create a scheduled report for time frame of 8:00 AM to 5:00 PM, and there is activity in your contact center between 4:46:00 PM and 4:59:59 PM, the data about that activity may not be aggregated prior 5:00 PM when the report is scheduled to generate. Instead, the report is generated after 5:15 PM, by which time the data for the last 15 minutes of the time range is included in the report.

**A scheduled Yesterday report works like a Last 24 hours report**

• Usually **Yesterday** specifies the previous calendar day while **Last 24 hours** specifies the 24 hours prior to the current time. However, if you schedule to run a **Yesterday** report, it will work like a **Last 24 hours** report.

**No message if a scheduled report doesn't run**

• If a scheduled report fails to run, you won't get any message in the Amazon Connect UI. You just won't see the report in the Amazon S3 location.

**Use your messaging system to email scheduled reports**

• To email a scheduled report to a list of co-workers, you need to generate the email manually using your messaging system. Amazon Connect doesn't provide an option to email the scheduled report automatically.
How to schedule a historical metrics report

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Create a new report and save it, or open a saved report.
3. Choose the down arrow next to Save in the top-right corner of the page and choose Schedule.
4. On the Recurrence tab, specify how often this report should be run (for example, weekly on Saturdays) and the range (for example, from midnight for the previous 5 days).
5. (Optional) On the Delivery Options tab, specify a prefix for the location in Amazon S3 for the report files.
6. Choose Create.

How to delete a scheduled report

To get to the page where you can delete a scheduled report, you need to create another temporary scheduled report.

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. On the navigation menu, choose Analytics and optimization, Saved reports.
3. On the View reports page, choose the Historical metrics tab.
4. Click or tap on the saved report that has been scheduled.
5. Choose the down arrow next to Save in the top-right corner of the page and choose Schedule.
6. Choose Create.
7. On the Schedule Report page, choose Delete next to the scheduled reports you want to delete.

For instructions on deleting saved reports, see How to delete saved reports.

Update a historical metrics report

After you save a report, you can update it at any time.

To update a historical metrics report

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Choose Analytics and optimization, Saved reports.
3. From the Historical metrics tab, choose the name of the report. Choose the gear icon, update the report settings as needed, and choose Apply.

4. To update the current report, choose Save. To save your changes to a new report, choose Save as.

**Download a historical metrics report**

You can download the data included in a report as a comma-separated value (CSV) file so you can use it with other applications. If there's no data for one of the selected metrics, the field in the downloaded CSV file contains a dash.

**To download a historical metrics report as a CSV file**

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Create a new report or open a saved report.
3. Choose the down arrow next to Save in the top-right corner of the page and choose Download CSV.
4. When prompted, confirm whether to open or save the file.

The following image shows metrics in a Queue table. All times in the online report are in hours:minutes:seconds (hh:mm:ss). Below the image of the Queue table, there is an image of the same data in a downloaded CSV file opened with Excel. All times in the downloaded report are in seconds.
You can convert the seconds to minutes using an Excel formula. Alternatively, if you have a short report, you can copy and paste the data from Amazon Connect to Excel and it will preserve the format.

**Interval downloaded in ISO date format**

The interval is downloaded in ISO date format, as shown in the following image. When you download a historical metrics report, the interval will be in ISO data format and won't match the UI. If needed, use Excel to convert it to the desired format.
Download all historical metric results

If you need to download more than a page or two of historical metrics, we recommend using the following steps:

1. Schedule the report to run as often as needed.
   
   For example, you might schedule the Login/Logout report to run daily at midnight.
2. The full report is saved to your Amazon S3 bucket.
3. Go to your Amazon S3 bucket and download the report.

To learn how scheduled reports work, see Schedule a historical metrics report.

Show agent queues in a Queues table

By default agent queues don't appear in a Queues table in a historical metrics report. You can choose to show them.

To show agent queues in a Queues table

1. In a historical metrics report, choose the Settings icon, as shown in the following image.
2. Choose **Filters**, **Show agent queues**, **Agent queues**, and then use the drop-down to choose the agent's queues you want to include in the table. These options are shown in the following image.

3. Choose **Apply**. The agent queues you selected appear in the Queues table in the historical metrics report.
How many contacts in queue on a specific date

The historical metrics reports don't provide a way for you to determine how many contacts were in queue on a specific date, at a specific time.

To get this information in a historical report, you need the help of a developer. The developer uses the **GetCurrentMetricData** API to store the data so you can look it up later.

Agent activity audit report

The agent activity audit is like a report version of the **agent event stream**. All of the data in this report is also in the agent event stream.

For example, if there's something in the audit report you want to recreate, or if you want to recreate a different time period, you can do so using the agent event stream.

Run the agent activity audit report

For a list of required permissions to perform this procedure, see [Permissions required to view historical metrics reports](#).

1. Log in to the Amazon Connect admin website at `https://instance name.my.connect.aws/`.
2. Choose **Analytics and optimization, Historical metrics, Agents, Agent activity audit**.
3. Choose the agent login, date, and timezone, and then choose **Generate Report**.
4. To download the results, choose **Download CSV**.

Status definitions

The following values may appear in the **Status** column on agent activity audit report.

- **Available**: The agent has set their status in the Contact Control Panel (CCP) to **Available**. Contacts can be routed to them.
- **Offline**: The agent has set their status in the Contact Control Panel (CCP) to **Offline**. Contacts cannot be routed to them.
- **Custom status**: The agent has set their status in the Contact Control Panel (CCP) to a custom status. Contacts cannot be routed to them.
- **Joining Customer**: The state between an inbound contact arriving in the flow and routing to the agent.
• **Connecting Agent**: The state between an inbound contact being routed to an agent and the agent receiving the contact.

• **Connected**: When an inbound contact has been established by the agent choosing **Accept** in their CCP.

• **Busy**: The agent is interacting with a customer.

• **Agent Disconnected**: When the agent doesn't choose **Accept** on the inbound contact in 20 seconds, or they choose **Reject**.

• **Calling Customer**: The state before an outbound call is established.

• **Contact Missed**: When the agent misses a contact.

• **Missed Call Agent**: When an agent accepts a callback, but they end the call before ringing the customer has finished.

• **Telecom issue**: When an outbound call is ended before the call is established. For example, there was an error with the agent's soft phone connection.

---

**Note**

If a status appears in your report but is not listed on this page, it is a custom status created by your organization. Contact your Amazon Connect admin to learn the definition.

---

**Permissions required to view agent activity audit reports**

To view real-time metrics reports, you need to be assigned to a security profile that has either the **Access metrics - Access** permission or the **Real-time metrics - Access** permission. Note the following behavior when you assign these permissions:

• When **Access metrics - Access** is selected, the **Real-time metrics**, **Historical metrics**, and **Agent activity audit** permissions are also automatically assigned.

• When **Access metrics - Access** is assigned, you have access to all real-time and historical metrics reports.
If only Agent activity audit - Access is selected, you have access to only agent activity audit report and no other analytics pages or reports. The following image shows the Analytics and Optimization section, with only Agent activity audit - Access selected.

Agent activity audit tag-based access control

You can use resource tags and access control tags to apply granular access to users for the agent activity audit report. For example, you can control who has access to view agent status history for specific users in the report. The following images provide example views of the agent activity audit report with and without tag-based access controls:

Without tag-based access controls, you see all agents:
By using tag-based access controls, you can see a limited set of agents:

Tag-based access controls are available for real-time metrics; however, they are not applicable to other historical metric reports or the login/logout report. For more information, please see [Real-time metrics tag-based access control](#).

Tag-based access controls enable you to configure granular access to specific resources based on assigned resource tags. You can configure tag based access controls via the API/SDK or within the Amazon Connect console (for supported resources). You must configure user resource tags and access control tags before tag-based access control is applied to users for the agent activity audit report. For more information, please see [Tagging resources in Amazon Connect](#) and [Tag-based access control](#).

**How To Enable Tag-based Access Control for Agent Activity Audit Report**

To use tags to control access to users for the agent activity audit report, you must first configure user resource tags and access control tags. After your resource tags and access control tags are configured, you need to apply the appropriate permissions.

After your resource tags, access control tags, and permissions have been appropriately configured, you will have access controls applied to users for the agent activity audit report.

For more information on tagging resources and tag-based access control in Amazon Connect, see [Tagging resources in Amazon Connect](#) and [Tag-based access control](#).

**Permissions**

To view agent activity audit reports with tag-based access controls applied, you need to be assigned to a security profile that has Access selected for Agent Activity Audit or has Access selected for Access metrics permission, along with access to the user resource. Note that if you enable Access metrics, then Real-time metrics, Historical Metrics, and Agent Activity Audit will
be filled in automatically, and you therefore will be enabling users to see all data for historical metrics for which tag-based access controls are not currently applied.

### Login/Logout reports

The Login/Logout report displays the login and logout information for the users in your contact center (for example, agents, managers, and administrators). For each user session, the login and logout times are displayed as a row in the report. You can use the report to determine the time users were logged in to Amazon Connect. The report also displays the amount of time for each session that user was logged in to Amazon Connect.

⚠️ **Important**

By default, when an agent closes their CCP window, they are not logged out. Unless you have customized your CCP for automatic logout, agents must choose the **Logout** button. Until they choose the **Logout** button, the Login/Logout report shows them as logged in.
Login/Loginout report limit: 10,000 rows

- If you try to generate a Login/Loginout report that has more than 10,000 rows, it won't complete.
- The Login/Loginout report page displays only 10,000.
- If you schedule a Login/Loginout report that contains more than 10,000 rows, the report will fail. In addition, no report output will be saved to your S3 bucket, and you cannot view the report.
- If you have a contact center with a lot of users, and your reports fail to complete, you can specify a shorter time range to reduce the size of the report generated, or apply filters to the report, such as routing profile and agent hierarchy. You can then use other filters to capture all of the login/logout data for your instance.

Required permissions to access the Login/Loginout report

Before you can generate a Login/Loginout report, you need the following permissions assigned to your security profile: Login/Loginout report - View.

By default, the Amazon Connect Admin security profile has these permissions.

For information about how to add more permissions to an existing security profile, see Update security profiles.
Generate a Login/Logout report

A Login/Logout report includes only login or logout actions by your users that occurred during the specified time range.

- If user logged in during the time range and did not log out, the report shows a login time but not a logout time.
- If the user logged in before the start of the time range, and then logged out during the time range, the report shows both the login and logout times even though the login occurred before the start of the time range. This is so you can view the duration of the user session associated with the most recent logout.

To generate a Login/Logout report

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/.
2. Choose Analytics and optimization, Login/Logout report.
3. On the Login/Logout report page, choose the Time range for the records to include in the report. Choose Custom time range to specify a range up to 7 days. This configuration is shown in the following image.
4. Choose the **Time zone** to use for your report.
5. To filter data included in the report, for **Filter by**, choose a value.
6. Choose **Generate report**, **Save**.
7. Provide a name for the report, and choose **Save**.

**Edit a Saved Login/Logout Report**

After you save your report, you can edit it at any time. When you open a saved report, the time frame and date range displayed show the date and time defined when you saved the report.

**To edit a saved Login/Logout report**

1. Log in to the Amazon Connect admin website at https://*instance name*.my.connect.aws/.
2. Choose **Analytics and optimization**, **Saved reports**.
3. Choose **Login/Logout report** and select the report to edit.
4. Update the **Time range**, **Time zone**, and **Filter by** settings.
5. To overwrite your existing report, choose **Save**.
6. To save the changes as a new report, choose Save, Save as. Provide a name for the report and choose Save as.

**Download a Login/Logout report as a CSV File**

When you have generated a report, you can download it as a comma-separated value (CSV) file so that you can use it other applications to work with the data, such as a spreadsheet or database.

**To download a report as a CSV file**

1. Open the report to download.
2. On the Login/Logout report page, at the top right corner, choose the Share report menu (arrow) next to Save.
3. Choose Download CSV. The file Login_Logout report.csv is downloaded to your computer.

**Share a Login/Logout report**

To make the report available to other people in your organization, you can share a report. People can access the report only if they have appropriate permissions in Amazon Connect.

**To share a Login/Logout report**

1. On the Login/Logout report page, at the top right corner, choose the Share report menu (arrow) next to Save.
2. Choose Share report.
3. To copy the URL to the report, choose Copy link address. You can send the URL to others in your organization by pasting the link into an email or other document.
4. To publish the report to your organization, for Publish report to organization, move the toggle to On.
5. Choose Save.
Schedule a Login/Logout report

To generate a report with the same settings on a regular basis, you can schedule the report to run daily or on specific days of the week. Note that scheduled Login/Logout reports work differently than Login/Logout reports you generate from the user interface for a specified time range.

Important things to know

- When you schedule a report, it is automatically published to your organization. Anyone with appropriate permissions can view the report. Users with all permissions for Login/Logout reports can also edit, schedule, or delete the report.
- For scheduled Login/Logout reports, the trailing window value is always the last 24 hours.
- A scheduled report always runs at 12AM on the day you select, in the time zone that you choose.

  For example, if you select Wednesday, the report runs at midnight Wednesday and does not include any data for Wednesday.
- Scheduled reports are saved as CSV files in your Amazon S3 bucket. The default time zone is UTC. To have your report run at 12AM in your local time, choose your time zone instead.
- To email a scheduled report to a list of co-workers, you need to generate the email manually using your messaging system. Amazon Connect doesn’t provide an option to email the scheduled report automatically.

How to schedule a Login/Logout report

1. If you already have a saved report to schedule open, skip to step 4. Otherwise, in the dashboard, choose Analytics and optimization, Saved reports.
2. Choose Login/Logout report.
3. Hover the mouse pointer over the row containing the name of the report to schedule, and choose the Schedule report icon.
4. On the Schedule report page, under Recurrence, for Generate this report, choose whether to generate the report Daily or Weekly.
5. If you choose Weekly, select the day or days of the week on which to run the report.
6. Choose the Time zone.
7. To add a prefix to the S3 path to the saved report, choose Delivery Options and enter a value in the Prefix field.
The prefix is added to the path between /Reports and the report name. For example: .../Reports/my-prefix/report-name-YYYY-MM-DD...

8. Choose Create.

After you schedule a report, you can change or delete the schedule for it at any time.

To edit or delete the schedule for a report

1. Follow the steps in the preceding section to open the Schedule report page.
2. To edit the schedule, choose Edit, update the Recurrence and Delivery Options as desired, and then choose Save.
3. To delete the schedule for the report, choose Delete, and then choose Delete again on the confirmation dialog.

Delete a Saved Login/Logout report

Too many reports in your report library? If you no longer want to use a saved report, you can delete it. When you delete a report, you are only deleting the settings for the report, not any reports that have already been generated using those settings. No CSV files created from a scheduled report are removed from your S3 bucket.

To delete a saved Login/Logout report

1. Open your Amazon Connect dashboard.
2. Choose Analytics and optimization, Saved reports.
3. Hover over the row for the report to delete, and choose the Delete icon.
4. Choose Delete again.

Tag-based access control

Amazon Connect does not currently support tag-based access controls for login/logout reports.
Amazon Connect agent event streams

Amazon Connect agent event streams are Amazon Kinesis data streams that provide you with near real-time reporting of agent activity within your Amazon Connect instance. The events published to the stream include these CCP events:

• Agent login
• Agent logout
• Agent connects with a contact
• Agent status change, such as to Available to handle contacts, or on Break or at Training.

You can use the agent event streams to create dashboards that display agent information and events, integrate streams into workforce management (WFM) solutions, and configure alerting tools to trigger custom notifications of specific agent activity. Agent event streams help you manage agent staffing and efficiency.

Contents

• Enable agent event streams
• Sample agent event stream
• Determine how long an agent spends doing ACW
• Agent event streams data model

Enable agent event streams

Agent event streams are not enabled by default. Before you can enable agent event streams in Amazon Connect, create a data stream in Amazon Kinesis Data Streams. Then, choose the Kinesis stream as the stream to use for agent event streams. Though you can use the same stream for both agent event streams and contact records, managing and getting data from the stream is much easier when you use a separate stream for each. For more information, see the Amazon Kinesis Data Streams Developer Guide.

When data is sent to Kinesis, the partition key used is the agent ARN. All events for a single agent are sent to the same shard, and any resharding events in the stream are ignored.
Note

If you enable server-side encryption for the Kinesis stream you select for agent event streams, Amazon Connect cannot publish to the stream. This is because it does not have permission to Kinesis kms:GenerateDataKey. To work around this, first enable encryption for scheduled reports or recordings of conversations. Next, create an AWS KMS key using KMS for encryption. Finally, choose the same KMS key for your Kinesis data stream that you use for encryption of scheduled reports or recordings of conversations so that Amazon Connect has appropriate permissions to encrypt data sent to Kinesis. For more information about creating a KMS key, see Creating Keys.

To enable agent event streams

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the console, choose the name in the Instance Alias column of the instance for which to enable agent event streams.
3. Choose Data streaming, then select Enable data streaming.
4. Under Agent Events, select the Kinesis stream to use, and then choose Save.

Sample agent event stream

In the following sample agent event stream, the agent is assigned to a routing profile that requires them to take both chats and calls. They can take one call, and up to three chats at a time.

Note

For how many chats and tasks an agent can take concurrently, see Amazon Connect service quotas.

```json
{
    "AWSAccountId": "012345678901",
    "CurrentAgentSnapshot":
    {
```
"AgentStatus": {
    "ARN": "example-ARN", //The ARN for the agent's current agent status (not for the agent).
    "Name": "Available", //This shows the agent status in the CCP is set to Available.
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
},
"NextAgentStatus": {
    "Name": "Lunch", //They set their next status, which pauses new contacts being routed to them while they finish their current contacts.
    "ARN": "example-ARN2", //The ARN of the agent status that the agent has set as their next status.
    "EnqueuedTimestamp": "2019-08-13T20:58:00.004Z", //When the agent set their next status and paused routing of incoming contacts.
}
"Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "AgentEventStreamTest",
    "LastName": "Agent",
    "RoutingProfile": {
        "Concurrency": [
            {
                "AvailableSlots": 3, //This shows the agent has 3 slots available.
                "Channel": "CHAT",
                "MaximumSlots": 3 //They aren't on any chats right now.
            },
            {
                "AvailableSlots": 1, //The agent has 1 slot available to take a call.
                "Channel": "VOICE",
                "MaximumSlots": 1 //The agent's routing profile allows them to take 1 call at a time.
            }
        ],
        "DefaultOutboundQueue": {
            "Channels": ["
"VOICE" //This outbound queue only works for calls.
],
"Name": "OutboundQueue"
},
"InboundQueues": [
{
  "Channels": [
    "VOICE",
    "CHAT"
  ],
  "Name": null //This queue has a name of "null" because it's an agent queue,
  //and agent queues don't have names.
},
{
  "Channels": [
    "CHAT",
    "VOICE"
  ],
  "Name": "Omni-channel-queue" //This inbound queue takes both chats and calls.
},
"Name": "AgentEventStreamProfile"
},
"Username": "aestest"
},
"Contacts": [ ]
},
"EventId": "EventId-1",
"EventTimestamp": "2019-08-13T20:58:44.031Z",
"EventType": "HEART_BEAT",
"PreviousAgentSnapshot": {
  "AgentStatus": {
    "Name": "Offline",
    "StartTimestamp": "2019-08-13T20:52:30.704Z"}}
{
    "Configuration": {
        "AgentHierarchyGroups": null,
        "FirstName": "AgentEventStreamTest",
        "LastName": "Agent",
        "RoutingProfile": {
            "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-
            cccc-dddd-111111111111/routing-profile/routing-profile-ARN",
            "Concurrency": [
                {
                    "AvailableSlots": 3,
                    "Channel": "CHAT",
                    "MaximumSlots": 3
                },
                {
                    "AvailableSlots": 1,
                    "Channel": "VOICE",
                    "MaximumSlots": 1
                }
            ],
            "DefaultOutboundQueue": {
                "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
                bbbb-cccc-dddd-111111111111/queue/queue-ARN",
                "Channels": [
                    "VOICE"
                ],
                "Name": "OutboundQueue"
            },
            "InboundQueues": [
                {
                    "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
                    bbbb-cccc-dddd-111111111111/queue/agent/agent-ARN",
                    "Channels": [
                        "VOICE",
                        "CHAT"
                    ],
                    "Name": null
                },
                {
                    "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaa-
                    bbbb-cccc-dddd-111111111111/queue/queue-ARN",
                    "Channels": [
                        "CHAT",
                        "VOICE"
                    ]
                }
            ]
        }
    }
}
Determine how long an agent spends doing ACW

There's no event in the agent event stream that tells you how long a contact is in the ACW state, and by extension how long an agent spends doing ACW. However, there's other data in the agent event stream that you can use to figure this out.

First, identify when the contact entered ACW. Here's how to do that:

1. Identify when the conversation between the contact and agent ENDED.
2. View the StateStartTimeStamp for the event.

For example, in the following agent event stream output, the contact enters ACW state at "StateStartTimeStamp": "2019-05-25T18:55:27.017Z".

### Tip

In the agent event stream, events are listed in reverse chronological order. We recommend reading through following examples by starting at the bottom of each example.
"Name": "Available",  //This just refers to the status that the agent sets manually in the CCP.
    It means they are ready to handle contacts, not say, on Break.
},
"Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "(Removed)",
    "LastName": "(Removed)",
    "RoutingProfile": {
        "DefaultOutboundQueue": {
            "Name": "BasicQueue"
        },
        "InboundQueues": [
            {
                "Name": "BasicQueue"
            },
            {
                "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
                "Name": "PrimaryQueue"
            }
        ],
        "Name": "Basic Routing Profile"
    },
    "Username": "(Removed)"
},
"Contacts": [
    {
        "Channel": "VOICE",
        "ContactId": "ContactId-1",  //This is the same contact the agent was working on when their state was CONNECTED (below).
        Since it's still the same contact but they aren't connected, we know the contact is now in ACW state.
        "InitialContactId": null,
"InitiationMethod": "OUTBOUND", //This indicates how the contact was initiated. OUTBOUND means the agent initiated contact with the customer.
"Queue": {
  "Name": "BasicQueue"
},
"QueueTimestamp": null,
"State": "ENDED", //This shows the conversation has ended.
"StateStartTimestamp": "2019-05-25T18:55:27.017Z" //This is the timestamp for the ENDED event (above), which is when the contact entered ACW state.
}
]
,
"EventId": "EventId-1",
"EventType": "STATE_CHANGE", //This shows that the state of the contact has changed; above we can see the conversation ENDED.
"PreviousAgentSnapshot": {
  "AgentStatus": {
    "Name": "Available", //This just refers to the status that the agent sets manually in the CCP.
  },
  "Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "(Removed)",
    "LastName": "(Removed)",
    "RoutingProfile": {
      "DefaultOutboundQueue": {
        "Name": "BasicQueue"
      },
      "InboundQueues": [
Next, determine when a contact left ACW. Here's how to do that:
1. Find where the `CurrentAgentSnapshot` has no contacts, and the state for the contact listed in the `PreviousAgentSnapshot` equals `ENDED`.

   Because a `STATE_CHANGE` event also occurs when the agent's configuration is changed, such as when they are assigned a different routing profile, this step confirms you have the right event.

2. Find where the `EventType` = "STATE_CHANGE".

3. View the `EventTimeStamp` for it.

For example, in the following agent event stream file, the contact left ACW at "EventTimestamp": "2019-05-25T18:55:32.022Z".

```json
{
  "AWSAccountId": "012345678901",
  "CurrentAgentSnapshot": {
    "AgentStatus": {
      "Name": "Available", //This just refers to the status that the agent sets manually in the CCP. It means they are ready to handle contacts, not say, on Break.
    },
    "Configuration": {
      "AgentHierarchyGroups": null,
      "FirstName": "(Removed)",
      "LastName": "(Removed)",
      "RoutingProfile": {
        "DefaultOutboundQueue": {
          "Name": "BasicQueue"
        },
        "InboundQueues": [
        {
```

Determine how long an agent spends doing ACW

1334
"Name": "BasicQueue"
},
{
  "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
  "Name": "PrimaryQueue"
}
],
"Name": "Basic Routing Profile"
},
"Username": "(Removed)"
},
"Contacts": [], //Since a contact isn't listed here, it means ACW for ContactId-1 (below) is finished, and the agent is ready for a new contact to be routed to them.
},
"EventId": "477f2c4f-cd1a-4785-b1a8-97023dc1229d",
"EventTimestamp": "2019-05-25T18:55:32.022Z", //Here's the EventTimestamp for the STATE_CHANGE event. This is when the contact left ACW.
"EventType": "STATE_CHANGE", //Here's the STATE_CHANGE
"PreviousAgentSnapshot": {
  "AgentStatus": {
    "Name": "Available", //This just refers to the status that the agent sets manually in the CCP.
    It means they were at work, not say, on Break.
},
"Configuration": {
  "AgentHierarchyGroups": null,
  "FirstName": "(Removed)",
  "LastName": "(Removed)",
  "RoutingProfile": {
    "DefaultOutboundQueue": {
      "Name": "BasicQueue"
Finally, to calculate the amount of time the contact was in the ACW state, and thus how long the agent spent working on it:

In this example, the agent spent 5.005 seconds doing ACW for ContactId-1.

**Agent event streams data model**

Agent event streams are created in JavaScript Object Notation (JSON) format. For each event type, a JSON blob is sent to the Kinesis data stream. The following event types are included in agent event streams:

- **LOGIN**—An agent login to the contact center.
- **LOGOUT**—An agent logout from the contact center.
- **STATE_CHANGE**—One of the following changed:
  - The agent changed their status in the Contact Control Panel (CCP). For example, they changed it from Available to on Break.
  - The state of the conversation between the agent and contact changed. For example, they were connected and then on hold.
  - One of the following settings changed in the agent's configuration:
    - Their routing profile
    - The queues in their routing profile
    - Auto-accept call
    - Sip address
    - Agent hierarchy group
    - Language preference setting in the CCP
- **HEART_BEAT**—This event is published every 120 seconds if there are no other events published during that interval.

**Note**

These events continue to be published up to an hour after an agent has logged off.

**Event Objects**

- **AgentEvent**
AgentEvent

The AgentEvent object includes the following properties:

AgentARN

The Amazon Resource Name (ARN) for the agent account.

Type: ARN

AWSAccountId

The 12-digit AWS account ID for the AWS account associated with the Amazon Connect instance.

Type: String

CurrentAgentSnapshot

Contains agent configuration, such as username, first name, last name, routing profile, hierarchy groups, contacts, and agent status.

Type: AgentSnapshot object

EventId

Universally unique identifier (UUID) for the event.

Type: String

EventTimestamp

A time stamp for the event, in ISO 8601 standard format.

Type: String (yyyy-mm-ddThh:mm:ss.sssZ)
**EventType**

The type of event.

Valid values: STATE_CHANGE | HEART_BEAT | LOGIN | LOGOUT

**InstanceARN**

Amazon Resource Name for the Amazon Connect instance in which the agent's user account is created.

Type: ARN

**PreviousAgentSnapshot**

Contains agent configuration, such as username, first name, last name, routing profile, hierarchy groups), contacts, and agent status.

Type: AgentSnapshot object

**Version**

The version of the agent event stream in date format, such as 2019-05-25.

Type: String

**AgentSnapshot**

The AgentSnapshot object includes the following properties:

**AgentStatus**

Agent status data, including:

- ARN—The ARN for the agent's current agent status (not for the agent).
- Name—This is the status of the agent that they manually set in the CCP, or that the supervisor manually changes in the real-time metrics report.

For example, their status might be **Available**, which means that they are ready for inbound contacts to be routed to them. Or it might be a custom status, such as Break or Training, which means that inbound contacts can't be routed to them BUT they can still make outbound calls.

- StartTimestamp—The timestamp in ISO 8601 standard format for the time at which the agent entered the status.
Type: String (yyyy-mm-ddThh:mm:ss.sssZ)

- Type—ROUTABLE, CUSTOM, or OFFLINE

Type: AgentStatus object.

NextAgentStatus

If the agent set a next agent status, the data appears here.

- ARN—The ARN of the agent status that the agent has set as their next status.
- Name—This is the name of the agent status that the agent has set as their next status.
- EnqueuedTimestamp—The timestamp in ISO 8601 standard format for the time at which the agent set their next status and paused routing of incoming contacts.

Type: String (yyyy-mm-ddThh:mm:ss.sssZ)

Type: NextAgentStatus object.

Configuration

Information about the agent, including:

- FirstName—The agent's first name.
- HierarchyGroups—The hierarchy group the agent is assigned to, if any.
- LastName—The agent's last name.
- RoutingProfile—The routing profile the agent is assigned to.
- Username—the agent's Amazon Connect user name.

Type: Configuration object

Contacts

The contacts

Type: List of Contact Objects object

Configuration

The Configuration object includes the following properties:

FirstName

The first name entered in the agent's Amazon Connect account.
Agent event streams data model

AgentHierarchyGroups
The hierarchy group, up to five levels of grouping, for the agent associated with the event.
Type: AgentHierarchyGroups object

LastName
The last name entered in the agent's Amazon Connect account.
Type: String
Length: 1-100

RoutingProfile
The routing profile assigned to the agent associated with the event.
Type: RoutingProfile object.

Username
The user name for the agent's Amazon Connect user account.
Type: String
Length: 1-100

Contact object
The Contact object includes the following properties:

ContactId
The identifier for the contact.
Type: String
Length: 1-256

InitialContactId
The original identifier of the contact that was transferred.
Type: String
Length: 1-256

**Channel**

The method of communication.

Valid values: VOICE, CHAT, TASKS

**InitiationMethod**

Indicates how the contact was initiated.

Valid values:

- **INBOUND**: The customer initiated voice (phone) contact with your contact center.
- **OUTBOUND**: An agent initiated voice (phone) contact with the customer, by using the CCP to call their number. This initiation method calls the `StartOutboundVoiceContact` API.
- **TRANSFER**: The customer was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.
- **CALLBACK**: The customer was contacted as part of a callback flow.

For more information about the InitiationMethod in this scenario, see [About queued callbacks in metrics](#).

- **API**: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the `StartOutboundVoiceContact` API, or it could be a live chat that was initiated by the customer with your contact center, where you called the `StartChatConnect` API.
- **QUEUE_TRANSFER**: While the customer was in one queue (listening to Customer queue flow), they were transferred into another queue using a flow block.
- **MONITOR**: A supervisor initiated monitor on an agent. The supervisor can silently monitor the agent and customer, or barge the conversation.

**Note**

This status shows only if you have opted into [Multi-Party Calls and Enhanced Monitoring](#).

- **DISCONNECT**: When a [Set disconnect flow](#) block is triggered, it specifies which flow to run after a disconnect event during a contact.
A disconnect event is when:

- A chat, or task is disconnected.
- A task is disconnected as a result of a flow action.
- A task expires. The task is automatically disconnected if it is not completed in 7 days.

If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

**State**

The state of the contact.

Valid values: INCOMING | PENDING | CONNECTING | CONNECTED | CONNECTED_ONHOLD | MISSED | REJECTED | ERROR | ENDED

**Note**

The REJECTED state does not apply to voice contacts. Rejected voice contacts appear as MISSED.

**StateStartTimestamp**

The time at which the contact entered the current state.

Type: String (yyyy-mm-ddThh:mm:ss.sssZ)

**ConnectedToAgentTimestamp**

The time at which the contact was connected to an agent.

Type: String (yyyy-mm-ddThh:mm:ss.sssZ)

**QueueTimestamp**

The time at which the contact was put into a queue.

Type: String (yyyy-mm-ddThh:mm:ss.sssZ)

**Queue**

The queue the contact was placed in.

Type: Queue object
**HierarchyGroup object**

The HierarchyGroup object includes the following properties:

**ARN**

The Amazon Resource Name (ARN) for the agent hierarchy.

Type: String

**Name**

The name of the hierarchy group.

Type: String

---

**AgentHierarchyGroups object**

The AgentHierarchyGroups object includes the following properties:

**Level1**

Includes details for Level1 of the hierarchy assigned to the agent.

Type: HierarchyGroup object

**Level2**

Includes details for Level2 of the hierarchy assigned to the agent.

Type: HierarchyGroup object

**Level3**

Includes details for Level3 of the hierarchy assigned to the agent.

Type: HierarchyGroup object

**Level4**

Includes details for Level4 of the hierarchy assigned to the agent.

Type: HierarchyGroup object

**Level5**

Includes details for Level5 of the hierarchy assigned to the agent.
Queue object

The Queue object includes the following properties:

ARN

The Amazon Resource Name (ARN) for the queue.

Type: String

Name

The name of the queue.

Type: String

Channels

The type of communication channel.

Type: List of Channel objects

RoutingProfile object

The RoutingProfile object includes the following properties:

ARN

The Amazon Resource Name (ARN) for the agent's routing profile.

Type: String

Name

The name of the routing profile.

Type: String

InboundQueues

The Queue objects associated with the agent's routing profile.
Type: List of Queue object

DefaultOutboundQueue

The default outbound queue for the agent's routing profile.

Type: Queue object

Concurrency

A list of concurrency information. Concurrency information objects have AvailableSlots (number), Channel (a channel object), and MaximumSlots (number) values.

Amazon Connect contact events

Amazon Connect allows you to subscribe to a near real-time stream of contact (voice calls, chat, and task) events (for example, call is queued) in your Amazon Connect contact center.

You can use contact events to create analytics dashboards to monitor and track contact activity, integrate into workforce management (WFM) solutions to better understand contact center performance, or to integrate applications that react to events (for example, call disconnected) in real-time.

Contents

- Subscribe to Amazon Connect contact events
- Contact events data model
- Contact timestamps
- Sample to stop streaming an event type
- Sample contact event for when a voice call is connected to an agent
- Sample contact event for when a voice call is disconnected
- Sample event for when contact properties are updated

Subscribe to Amazon Connect contact events

Amazon Connect contact events are published using Amazon EventBridge, and can be enabled in a couple of steps for your Amazon Connect instance in the Amazon EventBridge console by creating
a new rule. Although events are not ordered, they have a timestamp which enables you to consume the data.

Events are emitted on a **best effort** basis.

To subscribe to Amazon Connect contact events:

1. In the Amazon EventBridge console, choose **Create rule**.
2. On the **Default rule detail** page, assign a name to the rule, choose **Rule with an event pattern**, and then choose **Next**, as shown in the following image.

![Create rule](image)

3. On the **Build event pattern** page, under **Event source**, verify that **AWS events or EventBridge partner events** is selected.
4. Under **Sample event type**, choose **AWS events**, and then choose **Amazon Connect Contact Event** from the dropdown box, as shown in the following image.

![Sample event](image)
5. For Creation method choose Use pattern form. In the Event pattern section, choose AWS services, Amazon Connect, Amazon Connect Contact Event, and then choose Next, as shown in the following image.

![Event pattern](image)

6. On the Select target(s) page, you can then select a target of your choice, which includes a Lambda function, SQS queue, or SNS topic. For information about configuring targets, Amazon EventBridge targets.

For more information about configuring rules, see Amazon EventBridge rules in the Amazon EventBridge User Guide.

Contact events data model

Contact events are generated in JSON. For each event type, a JSON blob is sent to the target of your choice, as configured in the rule. The following contact events are available:

- INITIATED - A voice call, chat, or task is initiated or transferred.
- CONNECTED_TO_SYSTEM - The contact has established media (for example, it was answered by a person or by voicemail). This event is generated for any of the AnsweringMachineDetectionStatus codes.

Note

This event is generated for outbound calls (including Amazon Connect outbound campaigns) tasks, and chats.

- CONTACT_DATA_UPDATED - One or more of the following contact properties were updated on a voice call, chat, or task: scheduled timestamp (task only), user-defined attributes, and if Contact Lens is enabled for a given contact.
- QUEUED - A voice call, chat, or task is queued to be assigned to an agent.
- CONNECTED_TO_AGENT - A voice call, chat, or task is connected to an agent.
- DISCONNECTED - A voice call, chat, or task is disconnected. For outbound calls, the dial attempt is not successful, the attempt is connected but the call is not picked up, or the attempt results in a SIT tone.

A disconnect event is when:
- A chat, or task is disconnected.
- A task is disconnected as a result of a flow action.
- A task expires. The task is automatically disconnected if it is not completed in 7 days.

Event Objects

- Contact event
- QueueInfo
- Campaign
Contact event

The Contact object includes the following properties:

**ContactId**

The identifier for the contact.

Type: String

Length: 1-256

**InitialContactId**

The identifier of the initial contact.

Type: String

Length: 1-256

**RelatedContactId**

The contactId that is related to this contact.

Type: String

Length: Minimum of 1. Maximum of 256.

**PreviousContactId**

The original identifier of the contact that was transferred.

Type: String

Length: 1-256

**Channel**

The type of channel.

Type: VOICE, CHAT, or TASK
**InstanceArn**

Amazon Resource Name (ARN) for the Amazon Connect instance in which the agent's user account is created.

Type: ARN

**InitiationMethod**

Indicates how the contact was initiated.

Valid values:

- **INBOUND**: The customer initiated voice (phone) contact with your contact center.

- **OUTBOUND**: Represents an agent-initiated outbound voice call from the Contact Control Panel (CCP). This initiation method calls the `StartOutboundVoiceContact` API.

- **TRANSFER**: The contact was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.

- **CALLBACK**: The customer was contacted as part of a callback flow. For more information about the InitiationMethod in this scenario, see About queued callbacks in metrics.

- **API**: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the `StartOutboundVoiceContact` API, or it could be a live chat that was initiated by the customer with your contact center, where you called the `StartChatContact` API, or it could be a tasks initiated by the customer by calling the `StartTaskContact` API.

- **QUEUE_TRANSFER**: While the contact is one queue, and was then transferred into another queue using a flow block.

- **EXTERNAL_OUTBOUND**: An agent initiated voice (phone) contact with an external participant to your contact center using either quick connect in the CCP or a flow block.

- **MONITOR**: A supervisor initiated monitor on an agent. The supervisor can silently monitor the agent and customer, or barge the conversation.

- **DISCONNECT**: When a Set disconnect flow block is triggered, it specifies which flow to run after a disconnect event.

A disconnect event is when:

- A chat, or task is disconnected.

- A task is disconnected as a result of a flow action.

- A task expires. The task is automatically disconnected if it is not completed in 7 days.
When the disconnect event occurs, the corresponding content flow runs. If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

**Disconnect reason code**

Indicates how the contact was terminated. This is available for the contacts of outbound campaigns in which the media connection failed.

Valid values:

- **OUTBOUND_DESTINATION_ENDPOINT_ERROR**: Current configurations do not allow this destination to be dialed (for example, calling an endpoint destination from an ineligible instance).
- **OUTBOUND_RESOURCE_ERROR**: Instance has insufficient permissions to make outbound calls or necessary resources were not found.
- **OUTBOUND_ATTEMPT_FAILED**: There was an unknown error, invalid parameter, or insufficient permissions to call the API.
- **EXPIRED**: Not enough agents available, or not enough telecom capacity for such calls.

**AnsweringMachineDetectionStatus**

Indicates how an outbound campaign call is actually disposed if the contact is connected to Amazon Connect.

Type: String

Valid values:

- **HUMAN_ANSWERED**: The number dialed was answered by a person.
- **VOICEMAIL_BEEP**: The number dialed was answered by voicemail with a beep.
- **VOICEMAIL_NO_BEEP**: The number dialed was answered by a voicemail with no beep.
- **AMD_UNANSWERED**: The number dialed kept ringing, but the call was not picked up.
- **AMD_UNRESOLVED**: The number dialed was connected but the answering machine detection could not determine whether the call was picked up by a person or voicemail.
- **AMD_NOT_APPLICABLE**: The call disconnected before ringing, and there was no media to detect.
- **SIT_TONE_BUSY**: The number dialed was busy
- **SIT_TONE_INVALID_NUMBER**: The number dialed was not a valid number.
- **SIT_TONE_DETECTED**: A special information tone (SIT) was detected.
- **FAX_MACHINE_DETECTED**: A fax machine was detected.
- **AMD_ERROR**: The number dialed was connected, but there was an error in answering machine detection.

**EventType**

The type of event published.

Type: String

Valid values: INITIATED, CONNECTED_TO_SYSTEM, CONTACT_DATA_UPDATED, QUEUED, CONNECTED_TO_AGENT, DISCONNECTED

**UpdatedProperties**

The type of property updated.

Type: String

Valid values: ScheduledTimestamp, UserDefinedAttributes, ContactLens.ConversationalAnalytics.Configuration

**AgentInfo**

The agent the contact was assigned to.

Type: AgentInfo object

**QueueInfo**

The queue the contact was placed in.

Type: QueueInfo object

**ContactLens**

Contact Lens information if Contact Lens is enabled on the flow.

Type: For more information about the ContactLens object, see the [UpdateContactRecordingBehavior](#) action in the *Flow language* section of the [Amazon Connect API Reference](#).
**SegmentAttributes**

A set of system defined key-value pairs stored on individual contact segments using an attribute map. The attributes are standard Amazon Connect attributes and can be accessed in flows. Attribute keys can include only alphanumeric, -, and _ characters.

This field can be used to show channel subtype. For example, `connect:Guide` or `connect:SMS`.

Type: SegmentAttributes

Members: SegmentAttributeName, SegmentAttributeValue

**QueueInfo**

The QueueInfo object includes the following properties:

**QueueArn**

The Amazon Resource Name (ARN) for the queue.

Type: String

**QueueType**

The type of queue.

Type: String

**Campaign**

Information associated with a campaign.

Type: Campaign object

**AgentInfo**

The AgentInfo object includes the following properties:

**AgentArn**

The Amazon Resource Name (ARN) for the agent account.

Type: ARN
HierarchyGroups

The agent hierarchy group for the agent.

Type: ARN

CustomerVoiceActivity

The `CustomerVoiceActivity` object includes the following properties:

**GreetingStartTimestamp**

The date and time that measures the beginning of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**GreetingEndTimestamp**

The date and time that measures the end of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

Contact timestamps

**InitiationTimestamp**

The date and time this contact was initiated, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**ConnectedToSystemTimestamp**

The date and time the customer endpoint connected to Amazon Connect, in UTC time.

**EnqueueTimestamp**

The date and time the contact was added to the queue, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**ConnectedToAgentTimestamp**

The date and time the contact was connected to the agent, in UTC time.
Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**DisconnectTimestamp**

The date and time that the customer endpoint disconnected from Amazon Connect, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**ScheduledTimestamp**

The date and time when this contact was scheduled to trigger the flow to run, in UTC time. This is supported only for the task channel.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**GreetingStartTimestamp**

The date and time that measures the beginning of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**GreetingEndTimestamp**

The date and time that measures the end of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**Sample to stop streaming an event type**

The following sample shows how to stop streaming a CONTACT_DATA_UPDATED event from Amazon Connect to EventBridge.

```json
{
    "source": ["aws.connect"],
    "detail-type": ["Amazon Connect Contact Event"],
    "detail": {
        "eventType": [
            "anything-but": ["CONTACT_DATA_UPDATED"]
        ]
    }
}
```
Sample contact event for when a voice call is connected to an agent

{
"initiationTimestamp":"2021-08-04T17:17:53.000Z",
"contactId":"11111111-1111-1111-1111-111111111111",
"channel":"VOICE",
"instanceArn":"arn:aws::connect:your-region:123456789012:instance/12345678-1234-1234-1234-123456789012",
"initiationMethod":"INBOUND",
"eventType":"CONNECTED_TO_AGENT",
"agentInfo":{
  "connectedToAgentTimestamp":"2021-08-04T17:29:09.000Z",
  "hierarchyGroups": {
    "level1": {
    },
    "level2": {
    },
    "level3": {
    },
    "level4": {
    },
    "level5": {
    }
  }
}
Sample contact event for when a voice call is disconnected

```json
{
  "version": "0",
  "id": "the event ID",
  "detail-type": "Amazon Connect Contact Event",
  "source": "aws.connect",
  "account": "111122223333",
  "time": "2021-08-04T17:43:48Z",
  "region": "your-region",
  "resources": [
    "arn:aws:...",
    "contactArn",
    "instanceArn"
  ],
  "detail": {
    "eventType": "DISCONNECTED",
    "contactId": "11111111-1111-1111-1111-111111111111",
    "initialContactId": "11111111-2222-3333-4444-555555555555",
    "previousContactId": "11111111-2222-3333-4444-555555555555",
    "channel": "Voice",
    "initiationMethod": "OUTBOUND",
    "initiationTimestamp": "2021-08-04T17:53:00Z",
    "connectedToSystemTimestamp": "2021-08-04T17:55.000Z",
    "disconnectTimestamp": "2021-08-04T17:37.000Z",
    "queueInfo": {
      "queueArn": "arn",
      "queueType": "type",
      "enqueueTimestamp": "2021-08-04T17:29:04.000Z"
    }
  }
}
```
Sample event for when contact properties are updated

{

"agentInfo": {
  "agentArn": "arn",
  "connectedToAgentTimestamp": "2021-08-04T17:29:09.000Z",
  "hierarchyGroups": {
    "level1": {
    },
    "level2": {
    },
    "level3": {
    },
    "level4": {
    },
    "level5": {
    }
  }
},

"CustomerVoiceActivity": {
  "greetingStartTimestamp": "2021-08-04T17:29:20.000Z",
  "greetingEndTimestamp": "2021-08-04T17:29:22.000Z"
}
}
Sample contact data updated event
Contact records data model

This article describes the data model for Amazon Connect contact records. Contact records capture the events associated with a contact in your contact center. Real-time and historical metrics are based on the data captured in the contact records.

Important things to know

- We continually release new features that result in the addition of new fields to the contact records data model. Any changes we make to the data model are backward compatible. When
you develop applications, we recommend that you build them to ignore the addition of new fields in the contact records data model. This will help ensure your applications are resilient.

- Amazon Connect delivers contact records at least once. Contact records may be delivered again for multiple reasons, such as new information arriving after initial delivery. For example, when you use `update-contact-attributes` to update a contact record, Amazon Connect delivers a new contact record. This contact record is available for 24 months from the time the associated contact was initiated.

If you're building a system that consumes contact record export streams, be sure to include logic that checks for duplicate contact records for a contact. Use the `LastUpdateTimestamp` property to determine if a copy contains new data than previous copies. Then use the `ContactId` property for deduplication.

- Every action taken on a unique contact generates an event. These events appear as a field or an attribute on the contact record. If the number of actions for a contact exceeds a threshold, such as an internal storage limit, then any actions that follow will not appear on that contact record.

- For the contact record retention period and maximum size of the attributes section of a contact record, see Amazon Connect feature specifications.

- For information about when a contact record is created (and thus can be exported or used for data reporting), see Events in the contact record.

- For a list of all contact attributes, including telephony call and case attributes, see List of available contact attributes and their JSONPath reference.

**Agent**

Information about the agent who accepted the incoming contact.

**AgentInteractionDuration**

The time, in whole seconds, that an agent interacted with a customer. For outbound calls, this is the time, in whole seconds, that an agent was connected to a contact, even if the customer is not present.

Type: Integer

Min value: 0
AfterContactWorkDuration

The difference in time, in whole seconds, between AfterContactWorkStartTimestamp and AfterContactWorkEndTimestamp.

Type: Integer

Min value: 0

AfterContactWorkEndTimestamp

The date and time when the agent stopped doing After Contact Work for the contact, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

AfterContactWorkStartTimestamp

The date and time when the agent started doing After Contact Work for the contact, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

ARN

The Amazon Resource Name of the agent.

Type: ARN

ConnectedToAgentTimestamp

The date and time the contact was connected to the agent, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

CustomerHoldDuration

The time, in whole seconds, that the customer spent on hold while connected to the agent.

Type: Integer

Min value: 0

DeviceInfo

Information about agent's device.
DeviceInfo

HierarchyGroups

The agent hierarchy groups for the agent.

Type: AgentHierarchyGroups

LongestHoldDuration

The longest time, in whole seconds, that the customer was put on hold by the agent.

Type: Integer

Min value: 0

NumberOfHolds

The number of times the customer was put on hold while connected to the agent.

Type: Integer

Min value: 0

RoutingProfile

The routing profile of the agent.

Type: RoutingProfile

Username

The username of the agent.

Type: String

Length: 1-100

stateTransitions

The state transitions of a supervisor.

Type: Array of stateTransitions.

AgentHierarchyGroup

Information about an agent hierarchy group.
**ARN**

The Amazon Resource Name (ARN) of the group.

Type: ARN

**GroupName**

The name of the hierarchy group.

Type: String

Length: 1-256

**AgentHierarchyGroups**

Information about the agent hierarchy. Hierarchies can be configured with up to five levels.

**Level1**

The group at level one of the agent hierarchy.

Type: AgentHierarchyGroup

**Level2**

The group at level two of the agent hierarchy.

Type: AgentHierarchyGroup

**Level3**

The group at level three of the agent hierarchy.

Type: AgentHierarchyGroup

**Level4**

The group at level four of the agent hierarchy.

Type: AgentHierarchyGroup

**Level5**

The group at level five of the agent hierarchy.
Type: AgentHierarchyGroup

ContactDetails

Contains user-defined attributes which are lightly typed within the contact.

This object is used only for task contacts. For voice or chat contacts, or for tasks that have contact attributes set with the flow block, check the ContactTraceRecord Attributes object.

ContactDetailsName

Type: String
Length: 1-128

ContactDetailsValue

Type: String
Length: 0-1024

ReferenceAttributeName

Type: String
Length: 1-128

ReferenceAttributesValue

Type: String
Length: 0-1024

ContactTraceRecord

Information about a contact.

Agent

If this contact successfully connected to an agent, this is information about the agent.

Type: Agent
AgentConnectionAttempts

The number of times Amazon Connect attempted to connect this contact with an agent.

Type: Integer

Min value: 0

Attributes

The contact attributes, formatted as a map of keys and values.

Type: Attributes

Members: AttributeName, AttributeValue

AWSAccountId

The ID of the AWS account that owns the contact.

Type: String

AWSClusterName

The record format version.

Type: String

Channel

How the contact reached your contact center.

Valid values: VOICE, CHAT, TASK

ConnectedToSystemTimestamp

The date and time the customer endpoint connected to Amazon Connect, in UTC time. For INBOUND, this matches InitiationTimestamp. For OUTBOUND, CALLBACK, and API, this is when the customer endpoint answers.

Type: String (yyyy-mm-ddThh:mm:ssZ)

ContactId

The ID of the contact.
Type: String
Length: 1-256

**CustomerEndpoint**

The customer or external third party participant endpoint.

Type: [Endpoint](#)

**CustomerVoiceActivity**

The `CustomerVoiceActivity` object includes the following properties:

**GreetingStartTimestamp**

The date and time that measures the beginning of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**GreetingEndTimestamp**

The date and time that measures the end of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

**DisconnectTimestamp**

The date and time that the customer endpoint disconnected from Amazon Connect, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**DisconnectReason**

Indicates how the contact was terminated. This data is currently available in the Amazon Connect contact record stream and [Contact details](#) page.

The disconnect reason may not be accurate when there are agent or customer connectivity issues. For example, if the agent is having connectivity issues, the customer might not be able to hear them ("Are you there?") and hang up. This would be recorded as CUSTOMER_DISCONNECT and not reflect the connectivity issue.
Type: String

Voice contacts can have the following disconnect reasons:

- CUSTOMER_DISCONNECT: Customer disconnected first.
- AGENT_DISCONNECT: Agent disconnected when the contact was still on the call.
- THIRD_PARTY_DISCONNECT: In a third-party call, after the agent has left, the third-party disconnected the call while the contact was still on the call.
- TELECOM_PROBLEM: Disconnected due to an issue with connecting the call from the carrier, network congestion, network error, etc.
- BARGED: manager disconnected the agent from the call.
- CONTACT_FLOW_DISCONNECT: Call was disconnected in a flow.
- OTHER: This includes any reason not explicitly covered by the previous codes. For example, the contact was disconnected by an API.

Outbound campaign voice contacts can have the following disconnect reasons:

- OUTBOUND_DESTINATION_ENDPOINT_ERROR: Current configurations do not allow this destination to be dialed (for example, calling an endpoint destination from an ineligible instance).
- OUTBOUND_RESOURCE_ERROR: Instance has insufficient permissions to make outbound calls or necessary resources were not found.
- OUTBOUND_ATTEMPT_FAILED: There was an unknown error, invalid parameter, or insufficient permissions to call the API.
- EXPIRED: Not enough agents available, or not enough telecom capacity for such calls.

Chats can have the following disconnect reasons:

- AGENT_DISCONNECT: Agent explicitly disconnects or rejects a chat.
- CUSTOMER_DISCONNECT: Customer explicitly disconnects.
- OTHER: Used only for error states such as message transport issues.

For many contacts, such as contacts ended by flows or APIs, there will not be any disconnect reason. In the contact record it will appear as null.

Tasks can have the following disconnect reasons:

- AGENT_DISCONNECT: Agent marked the task as complete.
• EXPIRED: Task expired automatically because it was not assigned or completed within 7 days.
• CONTACT_FLOW_DISCONNECT: Task was disconnected or completed by a flow.
• API: The StopContact API was called to end the task.
• OTHER: This includes any reason not explicitly covered by the previous codes.

**AnsweringMachineDetectionStatus**

Indicates how an outbound campaign call is actually disposed if the contact is connected to Amazon Connect.

Valid values:

• HUMAN_ANSWERED: The number dialed was answered by a person.
• VOICEMAIL_BEEP: The number dialed was answered by voicemail with a beep.
• VOICEMAIL_NO_BEEP: The number dialed was answered by a voicemail with no beep.
• AMD_UNANSWERED: The number dialed kept ringing, but the call was not picked up.
• AMD_UNRESOLVED: The number dialed was connected but the answering machine detection could not determine whether the call was picked up by a person or voicemail.
• AMD_NOT_APPLICABLE: The call disconnected before ringing, and there was no media to detect.
• SIT_TONE_BUSY: The number dialed was busy
• SIT_TONE_INVALID_NUMBER: The number dialed was not a valid number.
• SIT_TONE_DETECTED: A special information tone (SIT) was detected.
• FAX_MACHINE_DETECTED: A fax machine was detected.
• AMD_ERROR: The number dialed was connected, but there was an error in answering machine detection.

**InitialContactId**

The identifier of the initial contact.

Type: String

Length: 1-256

**InitiationMethod**

Indicates how the contact was initiated.
Valid values:

- **INBOUND**: The customer initiated voice (phone) contact with your contact center.
- **OUTBOUND**: An agent initiated voice (phone) contact with the customer, by using the CCP to call their number. This initiation method calls the `StartOutboundVoiceContact` API.
- **TRANSFER**: The customer was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new CTR being created.
- **CALLBACK**: The customer was contacted as part of a callback flow.

For more information about the `InitiationMethod` in this scenario, see `About queued callbacks in metrics`.

- **API**: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the `StartOutboundVoiceContact` API, or it could be a live chat that was initiated by the customer with your contact center, where you called the `StartChatConnect` API.
- **QUEUE_TRANSFER**: While the customer was in one queue (listening to Customer queue flow), they were transferred into another queue using a flow block.
- **EXTERNAL_OUTBOUND**: An agent initiated voice (phone) contact with an external participant to your contact center using either quick connect in the CCP or a flow block.
- **MONITOR**: A supervisor initiated monitor on an agent. The supervisor can silently monitor the agent and customer, or barge the conversation.
- **DISCONNECT**: When a `Set disconnect flow` block is triggered, it specifies which flow to run after a disconnect event during a contact.

A disconnect event is when:

- A chat, or task is disconnected.
- A task is disconnected as a result of a flow action.
- A task expires. The task is automatically disconnected if it is not completed in 7 days.

If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

**InitiationTimestamp**

The date and time this contact was initiated, in UTC time. For **INBOUND**, this is when the contact arrived. For **OUTBOUND**, this is when the agent began dialing. For **CALLBACK**, this is when the callback contact was created. For **EXTERNAL_OUTBOUND**, this is when the agent started dialing
the external participant. For MONITOR, this is when the manager started listening to a contact. For TRANSFER and QUEUE_TRANSFER, this is when the transfer was initiated. For API, this is when the request arrived.

Type: String (yyyy-mm-ddThh:mm:ssZ)

InstanceARN

The Amazon Resource Name of the Amazon Connect instance.

Type: ARN

LastUpdateTimeStamp

The date and time this contact was last updated, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

MediaStreams

The media streams.

Type: Array of MediaStream

NextContactId

If this contact is not the last contact, this is the ID of the next contact.

Type: String

Length: 1-256

PreviousContactId

If this contact is not the first contact, this is the ID of the previous contact.

Type: String

Length: 1-256

Queue

If this contact was queued, this is information about the queue.

Type: QueueInfo
Campaign

Information associated with a campaign.

Type: Campaign object

Recording

If recording was enabled, this is information about the recording.

Type: RecordingInfo

Recordings

If recording was enabled, this is information about the recording.

Type: Array of RecordingsInfo

Note

The first recording for a contact will appear in both the Recording and Recordings sections of the contact record.

RelatedContactId

If this contact is associated with another contact, this is the identifier of the related contact.

Type: String

Length: 1-256.

ScheduledTimestamp

The date and time when this contact was scheduled to trigger the flow to run, in UTC time. This is supported only for the task channel.

Type: String (yyyy-mm-ddThh:mm:ssZ)

SegmentAttributes

A set of system defined key-value pairs stored on individual contact segments using an attribute map. The attributes are standard Amazon Connect attributes and can be accessed in flows. Attribute keys can include only alphanumeric, -, and _ characters.
This field can be used to show channel subtype. For example, `connect:Guide` or `connect:SMS`.

Type: SegmentAttributes

Members: SegmentAttributeName, SegmentAttributeValue

**SystemEndpoint**

The system endpoint. For **INBOUND**, this is the phone number that the customer dialed. For **OUTBOUND** and **EXTERNAL_OUTBOUND**, this is the outbound caller ID number assigned to the outbound queue that is used to dial the customer. For callback, this shows up as Softphone for calls handled by agents with softphone.

Type: [Endpoint](#)

**TransferCompletedTimestamp**

If this contact was transferred out of Amazon Connect, the date and time the transfer endpoint was connected, in UTC time.

Type: String (`yyyy-mm-ddThh:mm:ssZ`)

**TransferredToEndpoint**

If this contact was transferred out of Amazon Connect, the transfer endpoint.

Type: [Endpoint](#)

**DeviceInfo**

Information about participant's device.

**PlatformName**

Name of the platform that the participant used for the call.

Type: String

Length: 1-128

**PlatformVersion**

Version of the platform that the participant used for the call.
Type: String
Length: 1-128

**OperatingSystem**

Operating system that the participant used for the call.

Type: String
Length: 1-128

**DisconnectDetails**

Information about the call disconnect experience.

**PotentialDisconnectIssue**

Indicates the potential disconnection issues for a call. This field is not populated if the service does not detect potential issues.

Type: String
Length: 0-128

Valid values:

- **AGENT_CONNECTIVITY_ISSUE**: Indicates potential issues with agent network connectivity.
- **AGENT_DEVICE_ISSUE**: Indicates problems with the customer hearing the agent due to potential issues with the agent's device such as their workstation, headset, or microphone.

**Endpoint**

Information about an endpoint. In Amazon Connect, an endpoint is the destination for a contact, such as a customer phone number, or a phone number for your contact center.

**Address**

The value for the type of endpoint. For TELEPHONE_NUMBER, the value is a phone number in E.164 format.
Type: String
Length: 1-256

Type
The endpoint type. Currently, an endpoint can only be a telephone number.
Valid values: TELEPHONE_NUMBER

ExternalThirdParty
Information about the External Third Party participant.

ExternalThirdPartyInteractionDuration
The time, in whole seconds, that the external participant interacted with the customer.
Type: Integer
Min value: 0

MediaStream
Information about the media stream used during the contact.

Type
Type: MediaStreamType
Valid values: AUDIO, VIDEO, CHAT

QualityMetrics
Information about the quality of the participant's media connection.

QualityScore
Number measuring the estimated quality of the media connection.
Type: Number
Min value: 1.00

Max val: 5.00

**PotentialQualityIssues**

List of potential issues causing degradation of quality on a media connection. If the service did not detect any potential quality issues the list is empty.

Type: StringArray

Valid values: Empty array or array with any of the following values: HighPacketLoss, HighRoundTripTime, HighJitterBuffer.

**QueueInfo**

Information about a queue.

**ARN**

The Amazon Resource Name of the queue.

Type: ARN

**DequeueTimestamp**

The date and time the contact was removed from the queue, in UTC time. Either the customer disconnected or the agent started interacting with the customer.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**Duration**

The difference in time, in whole seconds, between EnqueueTimestamp and DequeueTimestamp.

Type: Integer

Min value: 0

**EnqueueTimestamp**

The date and time the contact was added to the queue, in UTC time.
Type: String (yyyy-mm-ddThh:mm:ssZ)

Name

The name of the queue.

Type: String

Length: 1-256

RecordingInfo

Information about a voice recording.

DeletionReason

If the recording was deleted, this is the reason entered for the deletion.

Type: String

Location

The location, in Amazon S3, for the recording.

Type: String

Length: 0-256

Status

The recording status.

Valid values: AVAILABLE | DELETED | NULL

Type

The recording type.

Valid values: AUDIO

RecordingsInfo

Information about a voice recording, chat transcript, or screen recording.
DeletionReason

If the recording/transcript was deleted, this is the reason entered for the deletion.

Type: String

FragmentStartNumber

The number that identifies the Kinesis Video Streams fragment where the customer audio stream started.

Type: String

FragmentStopNumber

The number that identifies the Kinesis Video Streams fragment where the customer audio stream stopped.

Type: String

Location

The location, in Amazon S3, for the recording/transcript.

Type: String

Length: 0-256

MediaStreamType

Information about the media stream used during the conversation.

Type: String

Valid values: AUDIO, VIDEO, CHAT

ParticipantType

Information about the conversation participant: whether they are an agent or contact. Following are the participant types:

- All
- Manager
- Agent
• Customer
• Thirdparty
• Supervisor

Type: String

**StartTimestamp**

When the conversation of the last leg of the recording started.

Type: String *(yyyy-mm-ddThh:mm:ssZ)*

**Status**

The status of the recording/transcript.

Valid values: AVAILABLE | DELETED | NULL

**StopTimestamp**

When the conversation of the last leg of recording stopped.

Type: String *(yyyy-mm-ddThh:mm:ssZ)*

**StorageType**

Where the recording/transcript is stored.

Type: String

Valid values: Amazon S3 | KINESIS_VIDEO_STREAM

**References**

Contains links to other documents that are related to a contact.

**Reference Info**

Name

Type: URL | ATTACHMENT | NUMBER | STRING | DATE | EMAIL

• When Type = ATTACHMENT, the record also has a Status field.
Status valid values: APPROVED | REJECTED

Value

RoutingProfile

Information about a routing profile.

ARN

The Amazon Resource Name of the routing profile.

Type: ARN

Name

The name of the routing profile.

Type: String

Length: 1-100

stateTransitions

Information about the state transitions of a supervisor.

stateStartTimestamp

The date and time when the state started in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

stateEndTimestamp

The date and time when the state ended in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

state

Valid values: SILENT_MONITOR | BARGE.
VoicIdResult

The latest Voice ID status.

Authentication

The voice authentication information for the call.

Type: Authentication

FraudDetection

The fraud detection information for the call.

Type: FraudDetection

GeneratedSpeakerId

The speaker identifier generated by Voice ID.

Type: String

Length: 25 characters

SpeakerEnrolled

Was the customer enrolled during this contact?

Type: Boolean

SpeakerOptedOut

Did the customer opt out during this contact?

Type: Boolean

Authentication

Information about Voice ID authentication for a call.

ScoreThreshold

The minimum authentication score required for a user to be authenticated.
Type: Integer
Min value: 0
Max value: 100

**MinimumSpeechInSeconds**

The number of seconds of speech used to authenticate the user.

Type: Integer
Min value: 5
Max value: 10

**Score**

The output of Voice ID authentication evaluation.

Type: Integer
Min value: 0
Max value: 100

**Result**

The string output of Voice ID authentication evaluation.

Type: String
Length: 1-32

Valid values: Authenticated | Not Authenticated | Not Enrolled | Opted Out | Inconclusive | Error

**FraudDetection**

Information about Voice ID fraud detection for a call.

**ScoreThreshold**

The threshold for detection of fraudsters in a watchlist that was set in the flow for the contact.
Type: Integer
Min value: 0
Max value: 100

**Result**

The string output of detection of fraudsters in a watchlist.
Type: String
Valid values: High Risk | Low Risk | Inconclusive | Error

**Reasons**

Contains fraud types: Known Fraudster and Voice Spoofing.
Type: List of String
Length: 1-128

**RiskScoreKnownFraudster**

The detection of fraudsters in a watchlist score for Known Fraudster category.
Type: Integer
Min value: 0
Max value: 100

**RiskScoreVoiceSpoofing**

The fraud risk score based on Voice Spoofing, such as playback of audio from Text-to-Speech systems recorded audio.
Type: Integer
Length: 3

**RiskScoreSyntheticSpeech (unused)**

This field is unused. This score is presented as a combined risk score for Voice Spoofing.
GeneratedFraudsterID

The fraudster ID if the fraud type is Known Fraudster.

Type: String
Length: 25 characters

WatchlistID

The fraudster watchlist that was set in the flow for the contact. Use for Known Fraudster Detection.

Type: String
Length: 22 characters

How to identify abandoned contacts

An abandoned contact refers to a contact that was disconnected by the customer while in queue. This means that they weren't connected to an agent.

The contact record for an abandoned contact has a Queue, and an Enqueue Timestamp because it was enqueued. It won't have a ConnectedToAgentTimestamp, or any of the other fields that populate only after the contact has been connected to an agent.

View a contact record in the UI

1. Do a contact search. A list of contact IDs will be returned.
2. Choose an ID to view the contact record for the contact.

The following image shows part of a contact record in the UI, for a chat conversation. Note the following:

- For chats, the initiation method is always API.
- The chat transcript is visible in the UI.
About agent status

Agents have a status. It’s manually set in the Contact Control Panel (CCP).

- When they’re ready to handle contacts, they set their status in the CCP to **Available**. This means inbound contacts can be routed to them.
- When agents want to stop taking inbound contacts, they set their status to a custom status that you create, such as **Break** or **Training**. They can also change their status to **Offline**.

**Tip**

Managers can manually change the agent’s status in the real-time metrics report.
The following diagram illustrates how the agent's status in the CCP stays constant while they are handling contacts, but in the real-time metrics report, the **Agent activity state** and the **Contact state** change.

For example, when the **Agent activity state** = *Incoming*, the **Contact state** = *Incoming contact*.

### About custom agent statuses

It's possible for agents to make outbound calls when their status in the CCP is set to a custom status. Technically, agents can make an outbound call when their CCP is set to **Offline**.

For example, an agent wants to make an outbound call to a contact. Because they don't want contacts to be routed to them during this time, they set their status to a custom status. So when you look at your real-time metrics report, you'll see the agent is simultaneously on **NPT** (the metric that indicates a custom status) and **On contact**, for example.

### About ACW (After contact work)

After a conversation between an agent and customer ends, the contact is moved into the ACW state.

When the agent finishes doing ACW for the contact, they click **Clear** to clear that slot so another contact can be routed to them.

To identify how long an agent spent on ACW for a contact:

- In the historical metrics report, **After contact work time** captures the amount of time each contact spent in ACW.
- In the agent event stream, you have to do some calculations. For more information, see **Determine how long an agent spends doing ACW**.
How do you know when an agent can handle another contact?

The Availability metric tells you when agents are finished with a contact and ready to have another one routed to them.

What appears in the real-time metrics report?

To find out what the agent status is in the real-time metrics report, look at the Agent Activity metric.

What appears in the agent event stream?

In the agent event stream you'll see the AgentStatus, for example:

```
{
    "AWSAccountId": "012345678901",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "Name": "Available", //When an agent sets their status to "Available" it means they are ready for // inbound contacts to be routed to them, and not say, at Lunch.
        }
    }
}
```

"We couldn't find this agent. Use the agent's user name to identify them."

On occasion, in the Contact summary the Agent field may say "We couldn't find this agent. Use the agent's user name to identify them." This message is shown in the following image of the Contact summary.
This is a generic message for contacts that did not get connected to an agent at the time. It usually means that the inbound call was not answered by the agent and the customer disconnected the call.

To confirm that the caller was never connected to an agent:

- **Disconnect reason** = **Customer disconnect**.
- No recording of the call is found for that contact ID.

To verify this behavior, call your contact center and disconnect after a period of time without an agent accepting the call.

**About contact states**

Contact states appear in two places: the real-time metrics reports and the agent event stream.

**Contact states in the agent event stream**

There are different events that can appear in the lifecycle of a contact. Each of these events appear in the agent event stream as a **State**. A contact can have the following states that appear in the agent event stream:

- **INCOMING** - This is specific to queued callbacks. The agent is presented with a callback.
- **PENDING** - This is specific to queued callbacks.
- **CONNECTING** - An inbound contact is being offered to the agent (it's ringing). The agent has not yet taken any action to accept or reject the contact, and they haven't missed it.
- CONNECTED - The agent has accepted the contact. Now the customer is in a conversation with the agent.
- CONNECTED_ONHOLD - They are in a conversation with the agent, and the agent has put the customer on hold.
- MISSED - The contact was missed by the agent.
- ERROR - This appears when, for example, the customer abandons the call during outbound whisper.
- ENDED - The conversation has ended, and the agent has started doing ACW for that contact.
- REJECTED - The contact was rejected by the agent or the customer abandoned the contact when it is connecting to the agent. This applies to chat and tasks.

Here's what the contact state looks like in the agent event stream:

```json
"Contacts": [  
   {  
     "Channel": "VOICE",  //This shows the agent and contact were talking on the phone.  
     "ContactId": "ContactId-1",  //This shows the agent was working with a contact identified as "ContactId-1".  
     "InitialContactId": null,  
     "InitiationMethod": "OUTBOUND",  //This shows the agent reached the customer by making an outbound call.  
     "Queue": {  
     },  
     "QueueTimestamp": null,  
     "State": "CONNECTED",  //Here's the contact state. In this case, it shows the contact was CONNECTED to the agent, instead of say, MISSED.  
     "StateStartTimestamp": "2019-05-25T18:55:21.011Z"  //This shows when the contact was connected to the agent.  
   }  
]
```
Events in the contact record

A contact record captures events associated with the contact in your contact center. For example, how long the contact lasted, when it started and stopped. For a list of all data that's captured in the contact record, see Contact records data model.

A contact record is opened for a customer when they are connected to your contact center. The contact record is completed when the interaction with the flow or agent ends (that is, the agent has completed the ACW and cleared the contact). This means it's possible for a customer to have multiple contact records.

The following diagram shows when a contact record is created for a contact. It shows three contact records for a contact:

- The first record is created when the contact is connected to Agent 1.
- The second record is created when the contact is transferred to Agent 2.
- The third record is created when the contact is connected to Agent 3 during a callback.

Each time a contact is connected to an agent, a new contact record is created. The contact records for a contact are linked together through the contactId fields: initial, next, and previous.
Tip
A contact is considered connected when a contact record is created. It’s possible a contact record can be created before a call is finished ringing for the caller, due to network conditions and PSTN event propagation.

About queued callbacks in metrics

This topic explains how queued callbacks appear in your real-time metrics reports and the contact record.

Tip
To see only the number of customers who are waiting for a call back, you need to create a queue that only takes callback contacts. To learn how to do this, see Set up routing. Currently there isn’t a way to see the phone numbers of the contacts waiting for callbacks.

1. Callbacks are initiated when the Transfer to queue block is triggered to create the callback in a callback queue. The following image of a flow shows the Transfer to queue block at the end of the flow.

2. After any initial delay is applied, the callback is put into the queue. It remains there until an agent is available and can be offered the contact. The following image shows the contact in the In queue column on the Real-time metrics page.
3. When the callback is connected to the agent, a new contact record is created for the contact. The following diagram shows three contact records. The third record is for the callback, connected to Agent 3.

4. The Initiation Timestamp in the callback contact record corresponds to when the callback is initiated in the flow, shown in step 1. The following image shows the Initiation Timestamp field on the Contact Record page.
How properties in the Transfer to Queue block affect this flow

The Transfer to queue block has the following properties, which affect how Amazon Connect handles the callback:

- **Initial delay**: This property affects when a callback is put in queue. Specify how much time has to pass between a callback contact being initiated in the flow, and the customer being put in queue for the next available agent. For more information, see How Initial delay affects Scheduled and In queue metrics.

- **Maximum number of retries**: If this is set to 2, then Amazon Connect tries to call the customer at most three times: the initial callback, and two retries.

- **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait before trying again.

How Initial delay affects Scheduled and In queue metrics

In the Transfer to queue block, the Initial delay property affects when a callback is put in queue. For example, assume Initial delay is set to 30 seconds. Here’s what appears in your real-time metrics report:
1. After 20 seconds, the callback has already been created, but it is not yet in queue because of the **Initial delay** setting. In the following image of the **Real-time metrics** page, **In queue** = 0 and **Scheduled** = 1.

![Real-time metrics screenshot](image1)

2. After 35 seconds, the callback contact has been placed in queue. In the following image, the callback is now **In queue**. It is no longer scheduled.

![Real-time metrics screenshot](image2)

3. Assume that after 40 seconds, an agent accepts the callback. The **In queue** column = 0, the **Scheduled** column = 0.

![Real-time metrics screenshot](image3)
What counts as a "Failed Callback Attempt"

If an agent doesn't accept an offered callback, it doesn't count as a failed callback attempt. Rather, the routing engine offers the callback to the next available agent, until an agent accepts.

A failed callback attempt would be along the lines of: an agent accepts a callback but then something goes wrong between then and the agent being joined to the customer.

The contact is considered to be in the callback queue until an agent accepts the offered callback contact.

Amazon Connect removes the callback from the queue when it's connected to the agent. At that time, Amazon Connect starts dialing the customer.

The following image shows what this looks like in a contact record:

- Dequeued At: The timestamp of when the callback was connected to the agent. It's also when Amazon Connect starts dialing the customer.

The enqueued time on the contact record for a particular callback leg corresponds to the amount of time that the contact was in queue before that particular callback attempt was made. This is not the total enqueued time across all contact records.

For example, an inbound call could be in queue for 5 minutes before a callback is scheduled. Then, after an initial delay of 10 seconds, the callback contact could be in a callback queue for 10 seconds before an agent accepts it. In this case, you would see two contact records:

1. The first contact record, with InitiationMethod=INBOUND, would have an enqueued time of 5 minutes.
2. The second contact record, with InitiationMethod=CALLBACK, would have an enqueued time of 10 seconds.

**Example: Metrics for a queued callback**

This topic shows an example queued callback flow and reviews how the contact records and times are set for it.

Assume we have set up the following flows:

- **Inbound flow** -- Runs when the customer calls the customer service number.
- **Customer queue flow** – Runs when the customer is waiting in queue. In this example, we build a flow that offers a callback to the customer. If the customer selects yes, this flow executes the Transfer to queue block to transfer the contact to the callback queue named CallbackQueue, with an initial delay of 99 seconds, and then hangs up.
- **Outbound whisper flow** -- When a queued callback is placed, the customer hears this after they pick up and before they connect to the agent. For example, "Hello, this is your scheduled callback..."
- **Agent whisper flow** -- The agent hears this right after they accept the contact, before they are joined to the customer. For example, "You are about to be connected to Customer John, who requested a refund for..."

In this example, John calls customer service. Here's what happens:

1. Inbound flow creates contact record-1:
   a. John calls customer service at 11:35. The Inbound flow runs and puts him in queue at 11:35.
   b. The Customer queue flow runs. At 11:37, John chooses to schedule a callback, so Amazon Connect initiates a callback contact at 11:37, before the inbound contact is disconnected.

2. Callback flow creates contact record-2:
   a. The callback contact was initiated at 11:37.
   b. Because the initial delay is 99 seconds, the callback contact is placed into CallbackQueue at 11:38:39, after the 99 seconds pass. Now the callback contact is offered to an available agent.
   c. After 21 seconds, an agent available at 11:39:00 and accepts the contact. The 10-second agent whisper flow is played to the agent.
d. After the agent whisper flow is complete, Amazon Connect calls John at 11:39:10. John picks up, and listens to the 15-second outbound whisper flow.

e. When the outbound whisper flow is complete, John is connected to the agent at 11:39:25. They talk until 11:45, and then John hangs up.

This scenario results in two contact records, which include the following metadata.

<table>
<thead>
<tr>
<th>Contact record-1</th>
<th>Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation Method</td>
<td>Inbound</td>
<td></td>
</tr>
<tr>
<td>Initiation Timestamp</td>
<td>11:35</td>
<td>The inbound contact is initiated in Amazon Connect.</td>
</tr>
<tr>
<td>ConnectedToSystem Timestamp</td>
<td>11:35</td>
<td>Because this is an inbound contact, InitiationTimestamp = ConnectedToSystemTimestamp.</td>
</tr>
<tr>
<td>Next Contact Id</td>
<td>points to contact record-2</td>
<td></td>
</tr>
<tr>
<td>Queue</td>
<td>InboundQueue</td>
<td></td>
</tr>
<tr>
<td>Enqueued Timestamp</td>
<td>11:35</td>
<td>The inbound contact is put in queue.</td>
</tr>
<tr>
<td>Dequeued Timestamp</td>
<td>11:37</td>
<td>Because no agent picked up, this is the same as DisconnectedTimestamp.</td>
</tr>
<tr>
<td>ConnectedToAgent Timestamp</td>
<td>N/A</td>
<td>John scheduled a callback before any agent could pick up.</td>
</tr>
<tr>
<td>Disconnected Timestamp</td>
<td>11:37:00</td>
<td>John was disconnected by flow.</td>
</tr>
<tr>
<td>contact record-2</td>
<td>Data</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>PreviousContactId</td>
<td>points to contact record-1</td>
<td></td>
</tr>
<tr>
<td>Initiation Timestamp</td>
<td>11:37</td>
<td>The callback contact is created in Amazon Connect.</td>
</tr>
<tr>
<td>Queue</td>
<td>CallbackQueue</td>
<td></td>
</tr>
<tr>
<td>Enqueued Timestamp</td>
<td>11:38:39</td>
<td>The contact was put into the CallbackQueue, after the 99-second initial delay completes.</td>
</tr>
<tr>
<td>Dequeued Timestamp</td>
<td>11:39:00</td>
<td>After 21 seconds, an agent accepts the contact.</td>
</tr>
<tr>
<td>Queue Duration</td>
<td>120 seconds</td>
<td>This is the initial delay (99 seconds), plus any additional time sitting in queue waiting for an agent to become available (21 seconds).</td>
</tr>
<tr>
<td>ConnectedToSystem Timestamp</td>
<td>11:39:10</td>
<td>John is called after the 10 second agent whisper flow completes.</td>
</tr>
<tr>
<td>ConnectedToAgent Timestamp</td>
<td>11:39:25</td>
<td>John and the agent are connected, after the 15 second outbound whisper flow completes.</td>
</tr>
<tr>
<td>Disconnected Timestamp</td>
<td>11:45</td>
<td>John hangs up.</td>
</tr>
</tbody>
</table>
Save custom reports

You can create custom real-time, historical, and login/logout reports that include only the metrics you're interested in. For instructions, see Create a real-time metrics report and Create a historical metrics report.

After you create a report, you can:

- **Save** the custom report and return to it later.
- **Share** a link to the custom report so only people in your organization who have the link AND who have the appropriate permissions in their security profile can access the report.
- **Publish** the report so everyone in your organization who has the appropriate permissions in their security profile can view the report.

**Personal saved reports count towards quota**

Personal saved reports count towards your service quota of reports per instance. For example, if you save a report every day, it will count towards your organization's number of saved reports for the instance.

For more information about quotas, see Amazon Connect service quotas.

**Create a naming convention**

All saved reports in your Amazon Connect instance must have a unique name. We recommend creating a naming convention that indicates who the owner of the report is. For example, use the team name or owner alias as the report suffix: Agent Performance - team name. That way, if the report is published, others will know who owns it.

If your organization needs to delete reports because you've reached the service quota for reports for your instance, a naming convention that includes the team or owner alias will help you track down the report owners to find out if the report is still needed.

**How to save reports**

1. Customize a real-time, historical, or login/logout report to include the metrics you want.
2. Choose **Save**. If you don't have permissions in your security profile to create reports, this button will be inactive.
3. Assign a unique name to the report.

**Tip**
We recommend establishing a naming convention for reports in your organization, especially published reports. This will help everyone identify who the owner is. For example, use the team name or owner alias as the report suffix: Agent Performance - *team name*.

4. To view the report at a later time, on the navigation menu, choose **Analytics and optimization, Saved reports**.

How to delete saved reports

1. Log in to the Amazon Connect admin website at https://*instance name*.my.connect.aws/.
   Use an Admin account or an account that has **Saved reports - Delete** permissions in its security profile.

2. On the navigation menu, choose **Analytics and optimization, Saved reports**.

3. Choose the **Historical metrics** tab.

4. Go to the row that has the report you want to delete, and choose the **Delete** icon, as shown in the following image. If you don't have permissions in your security profile to delete reports, this option won't be available.
Share custom reports

You can only share reports that you create and save. This means you need the following permissions in your security profile to share reports: **Access metrics** - **Access** and **Saved reports** - **Create**. The following image shows the **Access metrics** - **Access** permissions on the security profiles page.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>Access</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Enable/Disable</th>
<th>Enable download button</th>
<th>Delete</th>
<th>Publish</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Historical metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent activity audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact search</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search contacts by conversation characteristics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search contacts by keywords</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure searchable contact attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To share reports

1. On the page of the report you want to share, choose the **Actions** dropdown menu and then choose **Share report**. The following image shows an example report named **Historical metrics: Test**, and the location of the **Share report** option in the **Actions** dropdown menu.
Or, from your list of saved reports, choose the **Share report** icon, as shown in the following image.

2. Choose **Copy link address** and choose **Save**, as shown in the following image. This saves the link to your clipboard. Paste this link into an email or other location to share the report.
You don't need to publish the report to your organization in order to share the link with specific people.

⚠️ **Important**
Anyone who has the link and the appropriate permissions can access the report.

### View a shared report

To view a report that someone has shared with you, you need the following:

- A link to the report.
- Permissions in your security profile:
  - **Access metrics**, if the report is a real-time or historical metrics report
  - **View Login/Logout report**, if the report is a login/logout report
  - **View Saved reports**

These permissions are shown in the following image of the **Analytics and Optimization** section of the security profiles page.
Tips for viewing a shared report

- Every time you want to view the shared report, you need to access it through the link that was shared with you.
- If you get a 505 error when you choose the link that was shared with you, it means you don't have permissions to view the report.
- There's no way to save the exact same report to your list of Saved reports. You can give the report a new name and save it to your list, but then it's a different report from the one that was shared with you. If the owner of original report makes changes, you won't see them in your renamed report.

Publish reports

After you create and save a custom report with the metrics you're interested in, you can publish it so everyone in your organization with the appropriate permissions can access the report.

After a report is published, people will be able to see the report in their list of Saved reports.

_tip_

We recommend establishing a naming convention for reports in your organization. When reports are published, this will help everyone identify who the owner is. For example, use the team name or owner alias as the report suffix: Agent Performance - _team name_.

Only people who have permissions in their security profile to **Create** and/or **Edit** saved reports will be able to change the published report and save their changes to the published version.

To publish a report

1. On the real-time metrics, historical metrics, login/logout report, or Saved reports page, choose **Share report**.
2. In the **Share report** dialog box, toggle **Publish report** to **On**, and then choose **Save**. This toggle is shown in the following image of the dialog box.
The report appears in the list of Saved reports for everyone who has appropriate permissions in their security profile.

3. To unpublish the report, move the toggle to Off.

The report is removed from everyone’s list of Saved reports.

**View published reports**

To view published reports, at minimum you need the following permissions in your security profile:

- **Access metrics**, if the report is a real-time or historical metrics report
- **View** Login/Logout report, if the report is a login/logout report
- **View** Saved reports

These permissions are shown in the following image of the **Analytics and Optimization** section of the security profiles page.
To view published reports

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an account that has the appropriate permissions.

2. On the navigation menu, choose Analytics and optimization, Saved reports. Published reports appear in your list automatically.

Manage saved reports (admin)

You can view and delete all saved reports in your instance, including reports that were not created by you or that are not currently published.

To do this, you need the Analytics and Optimization - Saved reports (admin) permission in your security profile.

View and delete reports

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an account that has Save reports (admin) - All in it's the security profile.

2. On the navigation menu, choose Analytics and Optimization, Saved reports.

3. On the View Reports page, choose All reports.
4. Use the filters to search by report name, report type, published status, and user.

5. To delete reports, select the reports by using the boxes on the left and then choose **Remove**, as shown in the following image.

![View Reports](image)

**Monitoring your instance using CloudWatch**

Amazon Connect sends data about your instance to CloudWatch metrics so that you can collect, view, and analyze CloudWatch metrics for your Amazon Connect virtual contact center. You can use this data to monitor key operational metrics and set up alarms. Data about your contact center is sent to CloudWatch every 1 minute.

When you view the CloudWatch metrics dashboard, you can specify the refresh interval for the data displayed. The values displayed in the dashboard reflect the values for the refresh interval you define. For example, if you set the refresh interval to 1 minute, the values displayed are for a minute period. You can select a refresh interval of 10 seconds, but Amazon Connect does not send data more often than every 1 minute. Metrics that are sent to CloudWatch are available for two weeks, and then discarded. To learn more about metrics in CloudWatch, see the [Amazon CloudWatch User Guide](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/).  

**Note**

If your Amazon Connect instance was created on or before October 2018, you need to provide Amazon Connect with permission to begin publishing chat metrics to your CloudWatch account. To do so, create an IAM policy with the following permission and attach it to the Amazon Connect service role. You can find the Amazon Connect service role on the **Account overview** page for your Amazon Connect instance.
Amazon Connect metrics sent to CloudWatch

The AWS/Connect namespace includes the following metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallsBreachingConcurrencyQuota</td>
<td>The total number of voice calls that exceeded the concurrent calls quota for the instance. For the total number of calls that breach the quota, take a look at the Sum statistic.</td>
</tr>
</tbody>
</table>

For example, assume your contact center experiences the following volumes, and your service quota is 100 concurrent calls:

- 0:00 : 125 concurrent calls. This is 25 over the quota.
- 0:04 : 135 concurrent calls. This is 35 over the quota.
- 0:10 : 150 concurrent calls. This is 50 over the quota.

CallsBreachingConcurrencyQuota = 110: the total number of voice calls that exceeded the quota between 0:00 and 0:10.

Unit: Count

Dimension:

- **InstanceId**: The ID of your instance
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CallbackNotDialableNumber</strong></td>
<td>The number of times a queued callback to a customer could not be dialed because the customer's number is in a country for which outbound calls are not allowed for the instance. The countries allowed for an instance are defined by the service quotas.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>ContactFlow</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>ContactFlowName</strong>: The name of your flow</td>
</tr>
<tr>
<td><strong>CallRecordingUploadError</strong></td>
<td>The number of call recordings that failed to upload to the Amazon S3 bucket configured for your instance. This is the bucket specified in <strong>Data Storage &gt; Call Recordings</strong> settings for the instance.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>CallRecordings</strong></td>
</tr>
<tr>
<td><strong>CallsPerInterval</strong></td>
<td>The number of voice calls, both inbound and outbound, received or placed per second in the instance.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>VoiceCalls</strong></td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ChatsBreachingActiveChatsQuota</td>
<td>The total number of valid requests made to start a chat that exceeded the concurrent active chats quota for the instance. For the total number of chats requests that breach the quota, take a look at the Sum statistic.</td>
</tr>
</tbody>
</table>

For example, assume your contact center experiences the following volumes, and your service quota is 2500 concurrent active chats:

- 0:00 : 2525 concurrent active chats. This is 25 over the quota.
- 0:04 : 2535 concurrent active chats. This is 35 over the quota.
- 0:10 : 2550 concurrent active chats. This is 50 over the quota.

ChatsBreachingActiveChatsQuota = 110: the total number of chats that exceeded the quota between 0:00 and 0:10.

Unit: Count

Dimensions:

- **InstanceId**: The ID of your instance
- **MetricGroup**: Chats
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| ConcurrentActiveChats        | The number of *concurrent active chats* in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active chats at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active chats are included, not only active tasks that are connected to agents. While all statistics are available in CloudWatch for concurrent active chats, you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here. Unit: Count Dimensions:  
  - **InstanceId**: The ID of your instance  
  - **MetricGroup**: Chats |
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConcurrentActiveChatsPerc</td>
<td>The percentage of the concurrent active chats service quota used in the instance. This is calculated by:</td>
</tr>
<tr>
<td>Percentage</td>
<td>• ConcurrentActiveChats / ConfiguredConcurrentActiveChatsLimit</td>
</tr>
<tr>
<td></td>
<td>Where ConfiguredConcurrentActiveChatsLimit is the Concurrent active chats per instance configured for your instance.</td>
</tr>
<tr>
<td></td>
<td>Unit: Percent (Output displays as an integer. For example, 1% of chats is shown as 1, not as 0.01.)</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>Chats</strong></td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConcurrentCalls</td>
<td>The number of concurrent active voice calls in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active calls at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active voice calls are included, not only active calls that are connected to agents.</td>
</tr>
<tr>
<td></td>
<td>While all statistics are available in CloudWatch for concurrent voice calls you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>VoiceCalls</strong></td>
</tr>
<tr>
<td>ConcurrentCallsPercentage</td>
<td>The percentage of the concurrent active voice calls service quota used in the instance. This is calculated by:</td>
</tr>
<tr>
<td></td>
<td>• ConcurrentCalls / ConfiguredConcurrentCallsLimit</td>
</tr>
<tr>
<td></td>
<td>Unit: Percent (output displays as a decimal)</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: <strong>VoiceCalls</strong></td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConcurrentTasks</td>
<td>The number of concurrent active tasks in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active tasks at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active tasks are included, not only active tasks that are connected to agents. While all statistics are available in CloudWatch for concurrent tasks you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Tasks</td>
</tr>
<tr>
<td>ConcurrentTasksPercentage</td>
<td>The percentage of the concurrent active tasks service quota used in the instance. This is calculated by:</td>
</tr>
<tr>
<td></td>
<td>• ConcurrentTasks / ConfiguredConcurrentTasksLimit</td>
</tr>
<tr>
<td></td>
<td>Where ConfiguredConcurrentTasksLimit is the <a href="#">Concurrent tasks per instance</a> configured for your instance.</td>
</tr>
<tr>
<td></td>
<td>Unit: Percent (output displays as a decimal)</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Tasks</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ContactFlowErrors</td>
<td>The number of times the error branch for a flow was run.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: ContactFlow</td>
</tr>
<tr>
<td></td>
<td>• <strong>ContactFlowName</strong>: The name of your flow</td>
</tr>
<tr>
<td>ContactFlowFatalErrors</td>
<td>The number of times a flow failed to execute due to a system error.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: ContactFlow</td>
</tr>
<tr>
<td></td>
<td>• <strong>ContactFlowName</strong>: The name of your flow</td>
</tr>
<tr>
<td>LongestQueueWaitTime</td>
<td>The longest amount of time, in seconds, that a contact waited in a queue. This is the length of time a contact waited in a queue during the refresh interval selected in the CloudWatch dashboard, such as 1 minute or 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Unit: Seconds</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Queue</td>
</tr>
<tr>
<td></td>
<td>• <strong>QueueName</strong>: The name of your queue</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| MissedCalls                           | The number of voice calls that were missed by agents during the refresh interval selected, such as 1 minute or 5 minutes. A missed call is one that is not answered by an agent within 20 seconds.  

To monitor the total missed calls in a given time period, take a look at the Sum statistic in CloudWatch.  

Unit: Count  
Dimensions:  
- **InstanceId**: The ID of your instance  
- **MetricGroup**: VoiceCalls |
| MisconfiguredPhoneNumber               | The number of calls that failed because the phone number is not associated with a flow.  

Unit: Count  
Dimensions:  
- **InstanceId**: The ID of your instance  
- **MetricGroup**: VoiceCalls |
| PublicSigningKeyUsage                 | The number of times a flow security key (public signing key) was used to encrypt customer input in a flow.  

Unit: Count  
Dimensions:  
- **InstanceId**: The ID of your instance  
- **SigningKeyId**: The ID of your signing key |
### Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QueueCapacityExceededError</strong></td>
<td>The number of calls that were rejected because the queue was full.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Queue</td>
</tr>
<tr>
<td></td>
<td>• <strong>QueueName</strong>: The name of your queue</td>
</tr>
<tr>
<td><strong>QueueSize</strong></td>
<td>The number of contacts in the queue. The value reflects the number of contacts in the queue at the time the dashboard is accessed, not for the duration of the reporting interval.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Queue</td>
</tr>
<tr>
<td></td>
<td>• <strong>QueueName</strong>: The name of your queue</td>
</tr>
<tr>
<td><strong>SuccessfulChatsPerInterval</strong></td>
<td>The number of chats successfully started in the instance for the defined interval.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>Dimensions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>InstanceId</strong>: The ID of your instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>MetricGroup</strong>: Chats</td>
</tr>
</tbody>
</table>

---

Amazon Connect metrics sent to CloudWatch

1418
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| TasksBreachingConcurrencyQuota | The total number of tasks that exceeded the concurrent tasks quota for the instance. For the total number of tasks that breach the quota, take a look at the Sum statistic.  

For example, assume your contact center experiences the following volumes, and your service quota is 2500 concurrent tasks:

- 0:00: 2525 concurrent tasks. This is 25 over the quota.
- 0:04: 2535 concurrent tasks. This is 35 over the quota.
- 0:10: 2550 concurrent tasks. This is 50 over the quota.

TasksBreachingConcurrencyQuota = 110: the total number of tasks that exceeded the quota between 0:00 and 0:10.  

Unit: Count  
Dimensions:
- **InstanceId**: The ID of your instance  
- **MetricGroup**: Tasks |
| TasksExpired | Tasks which have expired after being active for 7 days.  

To monitor the total number of tasks that have expired in a given time period, take a look at the Sum statistic in CloudWatch.  

Unit: Count  
Dimensions:
- **InstanceId**: The ID of your instance  
- **MetricGroup**: Tasks  
- **ContactId**: The ID of the task contact |
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| TasksExpiryWarningReached      | Tasks that have been active for 6 days 22 hours and reached expiry warning limit. To monitor the total number of tasks that have reached expiry warning limit in a given time period, take a look at the Sum statistic in CloudWatch. Unit: Count Dimensions:  
  - **InstanceId**: The ID of your instance  
  - **MetricGroup**: Tasks  
  - **ContactId**: The ID of the task contact |
| ThrottledCalls                 | The number of voice calls that were rejected because the rate of calls per second exceeded the maximum supported quota. To increase the supported rate of calls, request an increase in the service quota for concurrent active calls per instance. To monitor the total throttled calls in a given time period, take a look at the Sum statistic in CloudWatch. Unit: Seconds Unit: Count Dimensions:  
  - **InstanceId**: The ID of your instance  
  - **MetricGroup**: VoiceCalls |
ToInstancePacketLossRate | The ratio of packet loss for calls in the instance, reported every 10 seconds. Each data point is between 0 and 100, which represents the ratio of packets lost for the instance.  
Unit: Percent  
Dimensions:  
- Participant: Agent  
- Type of Connection: WebRTC  
- Instance ID: The ID of your instance  
- Stream Type: Voice

Amazon Connect CloudWatch metrics dimensions

In CloudWatch, a dimension is a name/value pair that uniquely identifies a metric. In the dashboard, metrics are grouped by dimension. When you view metrics in the dashboard, only metrics with data are displayed. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard.

The following dimensions are used in the CloudWatch dashboard for Amazon Connect metrics.

Flow metrics dimension

Note

If a flow has a dimension name in non-ASCII characters, you won't be able to see it in CloudWatch.

Filters metric data by flow. Includes the following metrics:

- ContactFlowErrors
- ContactFlowFatalErrors
- PublicSigningKeyUsage
Contact metrics dimension

Filters metric data by contacts. Includes the following metrics:

- TasksExpiryWarningReached
- TasksExpired

Instance metrics dimension

Filters meta data by instance. Includes the following metrics:

- CallsBreachingConcurrencyQuota
- CallsPerInterval
- CallRecordingUploadError
- ChatsBreachingActiveChatQuota
- ConcurrentActiveChats
- ConcurrentActiveChatsPercentage
- ConcurrentCalls
- ConcurrentCallsPercentage
- ConcurrentTasks
- ConcurrentTasksPercentage
- MisconfiguredPhoneNumbers
- MissedCalls
- SuccessfulChatsPerInterval
- TasksBreachingConcurrencyQuota
- ThrottledCalls

Instance ID, Participant, Stream Type, Type of Connection

Filters metric data by connection. Includes the following metrics:

- ToInstancePacketLossRate
Queue metrics dimension

Note
If a queue has a dimension name in non-ASCII characters, you won't be able to see it in CloudWatch.

Filters metric data by queue. Includes the following metrics:

- CallBackNotDialableNumber
- LongestQueueWaitTime
- QueueCapacityExceededError
- QueueSize

Amazon Connect Voice ID metrics sent to CloudWatch

The VoiceID namespace includes the following metrics.

RequestLatency
The elapsed time for the request.

- Frequency: 1 minute
- Unit: Milliseconds
- Dimension: API

UserErrors
The number of Error counts due to bad requests from user.

- Frequency: 1 minute
- Unit: Count
- Dimension: API

SystemErrors
The number of Error counts due to internal service error.
Throttles

The number of requests that are rejected due to exceeding the max rate allowed for sending requests.

Frequency: 1 minute
Unit: Count
Dimension: API

ActiveSessions

The number of active sessions in the domain. Active sessions are sessions that are in pending or ongoing status.

Frequency: 1 minute
Unit: Count
Dimension: Domain

ActiveSpeakerEnrollmentJobs

The number of active Batch Enrollment Jobs in the domain. Active Jobs are those which are in Pending or InProgress status.

Frequency: 15 minutes
Unit: Count
Dimension: Domain

ActiveFraudsterRegistrationJobs

The number of active Batch Registration Jobs in the domain. Active Jobs are those which are in Pending or InProgress status.

Frequency: 15 minutes
Speakers

The number of Speakers in the domain.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

Fraudsters

The number of Fraudsters in the domain.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

Amazon Connect Voice ID metrics dimensions

The following dimensions are used in the CloudWatch dashboard for Amazon Connect Voice ID metrics. When you view metrics in the dashboard, only metrics with data are displayed. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard.

API metrics dimension

This dimension limits the data to one of the following Voice ID operations:

- DeleteFraudster
- EvaluateSession
- ListSpeakers
- DeleteSpeaker
- OptOutSpeaker
Domain metrics dimension

The Voice ID domain where the enrollment, authentication or registration is conducted.

Amazon AppIntegrations metrics sent to CloudWatch

The AWS/AppIntegrations namespace includes the following metrics.

**RecordsDownloaded**

The number of records that were successfully downloaded as part of an AppFlow flow execution for a data integration.

- Frequency: 1 minute
- Unit: Count
- Valid Statistics: Maximum, Sum, Minimum, Average

**RecordsFailed**

The number of records that failed to download as part of an AppFlow flow execution for a data integration.

- Frequency: 1 minute
- Unit: Count
- Valid Statistics: Maximum, Sum, Minimum, Average

**DataDownloaded**

The number of bytes that were successfully downloaded as part of an AppFlow flow execution for a data integration.

- Frequency: 1 minute
- Unit: Bytes
- Valid Statistics: Maximum, Sum, Minimum, Average

**DataProcessingDuration**

The time it took to process and download data as part of a single AppFlow flow execution for a data integration.
EventsReceived

The number of events that were successfully emitted from your third-party source application (Salesforce, Zendesk) and received on your event bus.

Frequency: 1 minute
Unit: Count
Valid Statistics: Maximum, Sum, Minimum, Average

EventsProcessed

The number of events that were successfully processed and forwarded to be evaluated against the rules you configured on an event integration.

Frequency: 1 minute
Unit: Count
Valid Statistics: Maximum, Sum, Minimum, Average

EventsThrottled

The number of events that were throttled because the rate of emitting events exceeded the maximum supported quota.

Frequency: 1 minute
Unit: Bytes
Valid Statistics: Maximum, Sum, Minimum, Average

EventsFailed

The number of events that failed to process due to malformed or unsupported third-party events, and other processing errors.

Frequency: 1 minute
Unit: Bytes

Valid Statistics: Maximum, Sum, Minimum, Average

**EventProcessingDuration**

The time it took to successfully process and forward an event to be evaluated against the rules you configured on an event integration.

Frequency: 1 minute

Unit: Milliseconds

Valid Statistics: Maximum, Sum, Minimum, Average

**Amazon AppIntegrations metric dimensions**

You can use the following dimensions to refine AppIntegrations metrics.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccountId</td>
<td>AWS account ID</td>
</tr>
<tr>
<td>ClientId</td>
<td>Service principal of the client</td>
</tr>
<tr>
<td>IntegrationARN</td>
<td>ARN of the event or data integration</td>
</tr>
<tr>
<td>IntegrationType</td>
<td>DataIntegration or EventIntegration</td>
</tr>
<tr>
<td>Region</td>
<td>Region of the data or event integration</td>
</tr>
</tbody>
</table>

**Amazon Connect Customer Profiles metrics**

The AWS/CustomerProfiles namespace includes the following metrics.

**Real-time export metrics sent to CloudWatch**

The two following metrics will be published to CloudWatch for every export task. These metrics will provide information on your export stream tasks and will allow you to configure your Kinesis...
streams based on your use case. In the case of being throttled, these metrics will enable you to provision your Kinesis stream to ensure delivery to your destination.

**EventsProcessed**

Number of records successfully streamed into a Kinesis Stream.

Unit: Count

**EventsThrottled**

Number of PutRecord attempts that encountered throttling exception.

Unit: Count

---

**Amazon Connect Customer Profiles metric dimensions**

You can use the following dimensions to refine Customer Profiles metrics.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td>Customer Profiles domain name</td>
</tr>
<tr>
<td>DestinationType</td>
<td>Type of destination. Available value is: Kinesis</td>
</tr>
<tr>
<td>DestinationName</td>
<td>Name of destination. Kinesis Data Streaming name for DestinationType: Kinesis</td>
</tr>
</tbody>
</table>

---

**Use CloudWatch metrics to calculate concurrent call quota**

⚠️ **Important**

The **ConcurrentCallsPercentage** calculation information is not the same as **ConcurrentTasksPercentage** and **ConcurrentChatPercentage**.

- The metrics emitted for **ConcurrentCallsPercentage** are in decimal and not multiplied by 100. The metric represents a percentage of your total quota.
- For **ConcurrentTasksPercentage** and **ConcurrentChatPercentage** the value is multiplied by 100. That gives you your total quota.
The metrics emitted are correct and there is no discrepancy in data.

Here's how to calculate your quota usage for concurrent calls.

With calls active in the system, look at **ConcurrentCalls** and **ConcurrentCallsPercentage**. Calculate how much of your quota has been used:

- \( \frac{\text{ConcurrentCalls}}{\text{ConcurrentCallsPercentage}} \)

For example, if **ConcurrentCalls** is 20 and **ConcurrentCallsPercentage** is 50, your quota usage is calculated as \( \frac{20}{50} = 0.40 \), which is **40% of your total quota**.

**It is INCORRECT to interpret this as 40 calls.**

**Use CloudWatch metrics to calculate concurrent active chats quota**

Here's how to calculate your quota for concurrent active chats.

With chats active in the system, look at **ConcurrentActiveChats** and **ConcurrentChatsPercentage**. Calculate the quota:

- \( \frac{\text{ConcurrentActiveChats}}{\text{ConcurrentActiveChatsPercentage}} \times 100 \)

For example, if **ConcurrentActiveChats** is 1000 and **ConcurrentActiveChatsPercentage** is 50, your quota is calculated as \( \frac{1000}{50} \times 100 = 2000 \). Your total quota is 2000 chats.

**Use CloudWatch metrics to calculate concurrent task quota**

Here's how to calculate your quota for concurrent tasks.

With tasks active in the system, look at **ConcurrentTasks** and **ConcurrentTasksPercentage**. Calculate the quota:

- \( \frac{\text{ConcurrentTasks}}{\text{ConcurrentTasksPercentage}} \times 100 \)

For example, if **ConcurrentTasks** is 20 and **ConcurrentTasksPercentage** is 50, your total quota is calculated as \( \frac{20}{50} \times 100 = 40 \). Your total quota is 40 tasks.
Logging Amazon Connect API calls with AWS CloudTrail

Amazon Connect is integrated with AWS CloudTrail, a service that provides a record of the Amazon Connect API calls that a user, role, or AWS service makes. CloudTrail captures Amazon Connect API calls as events. All public Amazon Connect APIs support CloudTrail.

Note

When you create or update the following resources by using the Amazon Connect admin website, the event is recorded in CloudTrail logging: quick connects, queues, and users. When you create or update the following resources, events are logged to CloudTrail only if the change is made using the AWS CLI or public APIs: hours of operation, flows, phone numbers, user hierarchies, agent status, and prompts.

Using the information that CloudTrail collects, you can identify a specific request to an Amazon Connect API, the IP address of the requester, the requester's identity, the date and time of the request, and so on. If you configure a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket. If you don't configure a trail, you can view the most recent events in Event History in the CloudTrail console.

For more information about CloudTrail, including how to configure and enable it, see Creating a Trail For Your AWS Account and AWS CloudTrail User Guide.

Amazon Connect information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in Amazon Connect, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Amazon Connect, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Creating a trail for your AWS account
• CloudTrail supported services and integrations
• Configuring Amazon SNS notifications for CloudTrail
• Receiving CloudTrail log files from multiple Regions
• Receiving CloudTrail log files from multiple accounts

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

• Whether the request was made with root or AWS Identity and Access Management (IAM) credentials.
• Whether the request was made with temporary security credentials for a role or federated user.
• Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Example: Amazon Connect log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the GetContactAttributes action.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAAAAA111111EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/John",
        "accountId": "123456789012",
        "accessKeyId": "AAAAAAA111111EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-08-15T06:40:14Z"
            }
        }
    }
}
```
Example: Amazon Connect Voice ID log file entries

Just like Amazon Connect, Voice ID is integrated with CloudTrail. When enabled, the service emits events for the Voice ID API calls made by a user, role, or an AWS service. You can reuse the same CloudTrail resources created for Amazon Connect, including the trail and the S3 bucket, to receive CloudTrail logs for Voice ID as well.

For security reasons, the sensitive fields which might contain PII information in the API requests and responses are redacted in the events.

The following example shows a CloudTrail log entry that demonstrates the CreateDomain action.
Example: Amazon Connect Voice ID log file entries
EventBridge events emitted by Amazon Connect

Amazon Connect emits a variety of events related to the contact center, including but not limited to the following types of events:

- **Contact events** - contact (voice calls, chat, and task) events.
- **Contact Lens events** - create rules that generate EventBridge events.
- **Voice ID events** - events for every transaction: enrollment, authentication, or detection of fraudsters in a watchlist. Events are sent to the EventBridge default event bus.

Analytics data lake (Preview)

You can use Analytics data lake as a central location to query various types of data from Amazon Connect. This data includes contact records and Contact Lens conversational analytics. Data is refreshed around every 24 hours. You can use the Analytics data lake to create custom reports or run SQL queries.

For information about related API actions, see Analytics data lake actions in the Amazon Connect API Reference.

Contents
• Access Analytics data lake
• Available tables

Access Analytics data lake

To access Analytics data lake, you must use the AWS CLI or AWS CloudShell, which is a browser-based, pre-authenticated shell that you can launch directly from the AWS Management Console. For information about how to use the AWS CLI, see AWS Command Line Interface. For more information about AWS CloudShell, see AWS CloudShell.

1. Submit a request to access the Analytics data lake preview. For information about how to request access, see Contact AWS.

The account team will respond to your access request and walk through the prerequisites for onboarding. When your access is confirmed, continue with the following steps.

2. Generate the generate Association api request file by running the aws connect batch-associate-analytics-data-set --generate-cli-skeleton input > input_batch_association.json command.

3. Open the JSON file in a text editor and enter the following:

  • **InstanceId** – Your Amazon Connect instance ID.
  • **DataSetID** – Enter the required tables. For more information about required tables, see Available tables.
  • **TargetAccountID** – Account ID to share data.

Here is an example of the JSON file.

```json
{
    "InstanceId": "your_instance_id",
    "DataSetIds": [
        "contact_trace_record_20230901", "contact_lens_speech_analytics_20230629"
    ],
    "TargetAccountID": "your_account_ID"
}
```
4. Associate analytics data lake to a single account by running the `aws connect batch-associate-analytics-data-set --cli-input-json file:///path/to/request/file` command (where this path is based on the location of the JSON file).

5. Open the AWS Management Console and accept the RAM invitation. For information about RAM, see [Accepting and rejecting resource share invitations](#).

6. Open the AWS Lake Formation console and create a linked table from a shared table. For information about creating a resource link, see [Creating a resource link](#).

7. Check if you have a database in AWS Lake Formation that can be used to store a linked table. To create a database in AWS Lake Formation, see [Creating a database](#).

8. In AWS Lake Formation, under **Tables**, shared tables are displayed after accepting the resource share. For example, `contact_statistic_record_20220101`.

9. Choose **Create table** to create a linked table.

10. On the **Table details** page in AWS Lake Formation, choose **Resource link**. Enter the shared table name under **Shared table**. For example, `contact_trace_record_20230901`.

11. Choose **Create**.

12. Open the Amazon Athena console [https://console.aws.amazon.com/athena/](https://console.aws.amazon.com/athena/), and run a query to check if the data with the shared instance_id is provided in the request file. For example, `select * from databasename.[linked table] limit 10`.

### Available tables

You must associate the following tables in your AWS account.

- Contacts Records (contact_trace_record_20230901). For more information, see [Contact records data model](#).
- Contact Lens Speech Analytics (contact_lens_speech_analytics_20230629). For more information, see [Real-time contact analysis segment streams data model](#).
- Contact Statistic Records (contact_statistic_record_20220101)
• Agent Queue Statistic Records (agent_queue_statistic_record_20220101)
• Agent Statistic Records (agent_statistic_record_20220101)
• Contact Evaluation Forms, Weekly (contact_evaluation_weekly_20230130), Queue Weekly (contact_evaluation_queue_weekly_20230130), and Agent Weekly (contact_evaluation_agent_weekly_20230130). For more information, see Example evaluation form output.
Customize the Amazon Connect Agent Workspace

This section explains how to customize the agent workspace and enable guided experiences.

Out-of-the-box, the agent workspace integrates all of your agent facing capabilities on one page. For example, when an agent accepts a call, chat, or task, they are given necessary information about the case and customer, plus real-time recommendations.

You can customize the agent workspace by enabling guided experiences, for example, and customizing the look and feel of the View resources in the agent workspace.

The following image shows the parts of the agent workspace.

1. The Contact Control Panel, which agents use to accept calls, chats, and tasks.
2. Real-time recommendations, powered by Amazon Q in Connect.
3. The case ID, and other info on the Cases tab, powered by Amazon Connect Cases.
5. Customer information on the Customer profile tab, powered by Amazon Connect Customer Profiles.
We also support integrating third-party applications, built by yourself or by vendors, into the agent workspace (Preview).
Step-by-step Guides

In the Amazon Connect agent workspace, you can create workflows that walk agents through custom UI pages that suggest what to do at a given moment during a customer interaction. You can create workflows that give your agents screen pops and single page forms, or you can created
detailed step-by-step guides that give your agents clear instructions on how to handle a particular use case. This experience is customizable, both in terms of the data you surface to your agent as well UI that they see.

To learn more about the possible UI configurations, see our interactive documentation.

To learn more about the pricing of step-by-step guides, choose the Guides tab on the Amazon Connect pricing page.

Overview

Agent facing workflows are configured by creating a flow that uses the Flow block: Show view. The Show view block determines what View to render in the agent’s UI while all pre-existing flow blocks can be used to create branching decision trees and send and receive data from external systems.

When mapping a view to a Show view block, you will be able to select from a list of pre-built Views. For more details on the views see Flow block: Show view.

Complex JSON Object support

The Show view block allows you to pass complex JSON objects between Amazon Connect agent workspaces and flows. Along with the Show view flow block, the Invoke AWS Lambda flow block is able to take JSON objects as input and output parameters. This allows you to pass larger quantities of data with fewer mapping steps required.

Enable step-by-step guides

The following steps allow you to provide your users with the ability to create guided experiences, and allow agents to interact with the experiences.

1. Enable admins to create visual flow

   Assign managers and business analysts to the Numbers and flows - Views security profile permission, as shown in the following image. This permission grants them the ability to configure step-by-step guides in flows.

   Since guides are created using flows, also assign the Flows - Edit, Create permissions so that they can create any type of flow.
2. Enable agents to view guides

Assign the Agent Applications - Custom views permission to agents. This enables them to see step-by-step guides in their agent workspace.

3. Increase your service quota for concurrent active chats per instance

The workflows that agents interact with run as chat contacts in Amazon Connect. We recommend that you increase your concurrent active chats per instance quota by the number of concurrent contacts you expect to have this feature enabled for.

For more information about quotas, see Amazon Connect quotas.
**View resource**

*Views* are UI templates that you can use to customize your agent's workspace. For example, you can use views to display contact attributes to an agent, provide forms for entering disposition codes, provide call notes, and present UI pages for walking agents through step-by-step guides.

Amazon Connect includes a set of views that you can add to your agent's workspace, and you can also create your own views using our public APIs.

When configuring views in flows using the **Show view** block, you can define both static and dynamic content for each view. The content for a specific view is composed of three key elements: a template, an input schema, and actions.

**Tip**

For the best data mapping experience, we recommend using the **Set JSON** option in the **Show view** block. All namespaces in flows can be referenced in the **Show View** block, including $.External, so you will be able to share data from external systems to your agent in whichever view you create. You can mix and match data from Amazon Connect and other sources in order to create a consolidated UI for your agent.

**Custom views**

Using APIs you can now create your own view resources. The View resource includes CloudFormation, CloudTrail, and Tagging support.

**Views API example**

**View description**

This view nests two cards within a container, and places a skip button to their right.
CLI command

```bash
aws connect create-view --name CustomerManagedCardsNoContainer \
--status PUBLISHED --content file://view-content.json \
--instance-id $INSTANCE_ID --region $REGION
```

**view-content.json**

```json
{
  "Template": "stringified-template-json",
  "Actions": ["CardSelected", "Skip"]
}
```

**Template JSON (not stringified)**

```json
{
  "Head": {
    "Title": "CustomerManagedFormView",
    "Configuration": {
      "Layout": {
        "Columns": ["10", "2"] // Default column width for each component is 12, which is also the width of the entire view.
      }
    }
  },
  "Body": [
    {
      "_id": "FormContainer",
      "Type": "Container",
      "Props": {},
      "Content": [
        {
          "_id": "cafe-card",
          "Type": "Card",
          "Props": {
            "Id": "CafeCard",
            "Heading": "Cafe Card",
```
"Icon": "Cafe",
"Status": "Status Field",
"Description": "This is the cafe card.",
"Action": "CardSelected" // Note that these actions also appear in the view-content.json file.
},
"Content": []
}
{
"_id": "no-icon-card",
"Type": "Card",
"Props": {
"Id": "NoIconCard",
"Heading": "No Icon Card",
"Status": "Status Field",
"Description": "This is the icon card.",
"Action": "CardSelected" // Note that these actions also appear in the view-content.json file.
},
"Content": []
}
{
"_id": "button",
"Type": "Button",
"Props": { "Action": "Skip" }, // Note that these actions also appear in the view-content.json file.
"Content": ["Skip"]
}
}

The View

Inputs

$.NoIconCardHeading indicates that an input for the field NoIconCardHeading is necessary to render the view.

Let's say NoIconCardHeading is set to No Icon Card.
View output example

Views output two main pieces of data: the Action taken, and the Output data.

When using a view with the Show view block, Action represents a branch, and Output data is set to the $.Views.ViewResultData flow attribute, as mentioned in the Show View block documentation.

**Scenario 1: Choose the Cafe Card**

```
"Action": "CardSelected"
"Output": {
    "Heading": "CafeCard",
    "Id": "CafeCard"
}
```

**Scenario 2: Choose the Skip Button**

```
"Action": "Skip"
"Output": {
    "action": "Button"
}
```
AWS managed views

Amazon Connect includes a set of views that you can add your agent's workspace. See the following for details on how to configure the different AWS managed views.

Detail view

The **Detail view** is for displaying information to the agent and providing them with a list of actions that they can take. A common use case of the **Detail view** is to surface a screen-pop to the agent at the start of a call.

- Actions in this view can be used to let an agent continue to the next step in a step-by-step guide or the actions can be used to invoke entirely new workflows.
- **Sections** is the only required component. It is where you can configure the body of the page you want to show to your agent.
- Optional components such as the **AttributeBar** are supported by this view.

Interactive documentation for **Detail view**

The following image shows an example of a **Detail view**. It has a page heading, description, and four examples.

<table>
<thead>
<tr>
<th>Example Attribute</th>
<th>Example Attribute</th>
<th>Example 3 Case:123456</th>
<th>Example 4 Attribute 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 1 Attribute 2</td>
<td>Example 2 Attribute 2</td>
<td>Example 3 Case:123456</td>
<td>Example 4 Attribute 2</td>
</tr>
</tbody>
</table>

**Sections**

- Content can be a static string, a TemplateString or a key-value pair. It can be a single data point or a list. For more information, see [TemplateString](#) or [AttributeSection](#).

**AttributeBar (Optional)**
• Optional, if provided will display the Attribute bar at the top of the view.

• Is a list of objects with required properties, **Label**, **Value**, and optional properties **LinkType**, **ResourceId**, **Copyable** and **Url**. For more information see, [Attribute](#).

  • **LinkType** can be external or connect application such as case.
    • When it is *external*, a user can navigate to a new browser page, which is configured with **Url**.
    • When it is *case*, a user can navigate to a new case detail on the Agent workspace, which configured with **ResourceId**.

  • **Copyable** allows users to copy the **ResourceId** by choosing it with your input device.

**Back (Optional)**

• Optional, but required if no actions are included. if provided will display the back navigation link.

• Is an object with a **Label** which will control what is displayed in the link text.

**Heading (Optional)**

• Optional, if provided will display **Text** as the title.

**Description (Optional)**

• Optional, if provided will display description text under the title.

**Actions (Optional)**

• Optional. If provided, will display a list of action at the bottom of the page.

**Input example**

```json
{
   "AttributeBar": [
       {"Label": "Example", "Value": "Attribute"},
       { "Label": "Example 2", "Value": "Attribute 3", "LinkType": "case", "ResourceId": "123456", "Copyable": true }
   ]
}
```
List view

The **List view** is for displaying information as a list of items with titles and descriptions. Items may also act as links with actions attached. It also optionally supports the standard back navigation and persistent context header.

Interactive [documentation](#) for List view

The following image shows an example of a List view. It has one column with three items in it.
Items

- Required, will display these items as a list.
- Each item may have a Heading, Description, Icon, and Id.
  - All properties are optional.
  - When Id is defined, the output will include the value as part of output.

AttributeBar (Optional)

- Optional, if provided will display the Attribute bar at the top of the view.
- Is a list of objects with required properties, Label, Value, and optional properties LinkType, Resourceld, Copyable and Url. For more information see, Attribute.
  - LinkType can be external or connect application such as case.
    - When it is external, a user can navigate to a new browser page, which is configured with Url.
    - When it is case, a user can navigate to a new case detail on the Agent workspace, which configured with Resourceld.
  - Copyable allows users to copy the Resourceld by choosing it with your input device.

Back (Optional)

- Optional, but required if no actions are included. if provided will display the back navigation link.
- Is an object with a Label which will control what is displayed in the link text.

Heading (Optional)

- Optional, if provided will display Text as the title.

SubHeading (Optional)

- Optional, if provided will display Text as the title of list.

Input data example
Output data example

```json
{
    Action: "ActionSelected",
    ViewResultData: {
```
Form view

The **Form view** allows you to provide your agents with input fields to gather required data and submit data to backend systems. This view consists of multiple *Sections* with a predefined *Section* style with a header. The body consists of various input fields arranged in a column or a grid layout format.

Interactive [documentation](#) for Form view

The following image shows an example of a Form view for a car rental reservation. It has location and date fields on it.
Sections

- Location in the **Form view** where input fields and display fields are located.
- **SectionProps**
  - **Heading**
    - Heading of the section
  - **Type**
    - Type of section
    - FormSection (forms handling user’s input) or DataSection (displaying a list of label and value)
  - **Items**
    - List of data based on the type. When Type is DataSection, the data should be attributes. If the Type is FormSection, the data should be form components.
  - **isEditable**
    - Show edit button at the header when it is provided when the section type is DataSection.
    - Boolean

Wizard (Optional)

- Display **ProgressTracker** at the left side of the view.
- Each item may have a Heading, Description, and Optional.
  - Heading is required

Back (Optional)

- Is an object or string with a Label which will control what is displayed in the link text.

Next (Optional)

- This action is used when the step is not the last step in steps.
- Is an object (FormActionProps) or string. For more information, see [FormActionProps](#).

Cancel (Optional)
• This action is used when the step is not the first step.
• Is an object (FormActionProps) or string. For more information, see FormActionProps.

Previous (Optional)
• This action is used when the step is not the first step.
• Is an object (FormActionProps) or string. For more information, see FormActionProps.

Edit (Optional)
• This action is shown when the section type is DataSection.
• Is an object (FormActionProps) or string. For more information, see FormActionProps.

AttributeBar (Optional)
• Optional, if provided will display the Attribute bar at the top of the view.
• Is a list of objects with required properties, Label, Value, and optional properties LinkType, ResourceId, Copyable and Url. For more information see, Attribute.
  • LinkType can be external or connect application such as case.
    • When it is external, a user can navigate to a new browser page, which is configured with Url.
    • When it is case, a user can navigate to a new case detail on the Agent workspace, which configured with ResourceId.
  • Copyable allows users to copy the ResourceId by choosing it with your input device.

Heading (Optional)
• String that displays as the page title.

SubHeading (Optional)
• Secondary message for the page.

ErrorText (Optional)
• Optional, shows server-side error messages.
• ErrorProps; String

**Input data example**

```json
{
  "AttributeBar": [
    {
      "Label": "Queue",
      "Value": "Sales"
    },
    {
      "Label": "Case ID",
      "Value": "1234567"
    },
    {
      "Label": "Case",
      "Value": "New reservation"
    },
    {
      "Label": "Attribute 3",
      "Value": "Attribute"
    }
  ],
  "Back": {
    "Label": "Back Home"
  },
  "Next": {
    "Label": "Confirm Reservation",
    "Details": {
      "endpoint": "awesomecustomer.com/submit"
    }
  },
  "Cancel": {
    "Label": "Cancel"
  },
  "Heading": "Modify Reservation",
  "SubHeading": "Cadillac XT5",
  "ErrorText": {
    "Header": "Modify reservation failed",
    "Content": "Internal Server Error, please try again"
  }
}
```
"Sections": [{
  "_id": "pickup",
  "Type": "FormSection",
  "Heading": "Pickup Details",
  "Items": [{
    "LayoutConfiguration": {
      "Grid": [
        {"colspan": {
          "default": "12",
          "xs": "6"
        }
      }
    },
    "Items": [{
      "Type": "FormInput",
      "Fluid": true,
      "InputType": "text",
      "Label": "Location",
      "Name": "pickup-location",
      "DefaultValue": "Seattle"
    }]
  }, {
    "LayoutConfiguration": {
      "Grid": [
        {"colspan": {
          "default": "6",
          "xs": "4"
        }
      }, {"colspan": {
          "default": "6",
          "xs": "4"
        }
      }
    },
    "Items": [{
      "Label": "Day",
      "Type": "DatePicker",
      "Fluid": true,
      "DefaultValue": "2022-10-10",
      "Name": "pickup-day"
    }, {"Label": "Time",
      "Type": "TimeInput"}
    ]
  }]
}]
"Fluid": true,
"DefaultValue": "13:00",
"Name": "pickup-time"
]}]
],
{
"_id": "dropoff",
"Heading": "Drop off details",
"Type": "FormSection",
"Items": [{
"LayoutConfiguration": {
  "Grid": [{
    "colspan": {
      "default": "12",
      "xs": "6"
    }
  }
  ]
},
"Items": [{
  "Label": "Location",
  "Type": "FormInput",
  "Fluid": true,
  "DefaultValue": "Lynnwood",
  "Name": "dropoff-location"
}]
}, {
  "LayoutConfiguration": {
    "Grid": [{
      "colspan": {
        "default": "6",
        "xs": "4"
      }
    }, {
      "colspan": {
        "default": "6",
        "xs": "4"
      }
    }
  ]
},
"Items": [{
  "Label": "Day",
  "Type": "DatePicker",
  "Fluid": true,
  "DefaultValue": "2022-10-15",
  "Name": "dropoff-day"
}]
}]}
Output data example

```json
{
    Action: "Submit",
    ViewResultData: {
        FormData: {
            "dropoff-day": "2022-10-15",
            "dropoff-location": "Lynnwood",
            "dropoff-time": "01:00",
            "pickup-day": "2022-10-10",
            "pickup-location": "Seattle",
            "pickup-time": "13:00"
        },
        StepName: "Pickup and drop off"
    }
}
```

Confirmation view

The **Confirmation view** is a page to show users after a form has been submitted or an action has been completed. In this pre-built template you can provide a summary of what has happened, any next steps, and prompts. The **Confirmation view** supports a persistent attribute bar, an icon/image, headline, and sub-headline, along with a back to home navigation button.

Interactive [documentation](#) for **Confirmation view**

The following image shows an example of a confirmation.
Next

- Required.
- Action button for next
  - Label - string label for the navigation button.

AttributeBar (Optional)

- Optional, if provided will display the Attribute bar at the top of the view.
- Is a list of objects with required properties, **Label**, **Value**, and optional properties **LinkType**, **ResourceId**, **Copyable** and **Url**. For more information see, **Attribute**.
  - **LinkType** can be external or connect application such as case.
• When it is *external*, a user can navigate to a new browser page, which is configured with *Url*.

• When it is *case*, a user can navigate to a new case detail on the Agent workspace, which configured with *ResourceId*.

• **Copyable** allows users to copy the *ResourceId* by choosing it with your input device.

**Heading (Optional)**

• String that displays as the page title.

**SubHeading (Optional)**

• Secondary message for the page.

**Graphic (Optional)**

• Displays an image

• Object with the following key:

  • Include - boolean, if this is true then the graphic will be included in the page.

**Input Data Example**

```json
{
    "AttributeBar": [
        { "Label": "Attribute1", "Value": "Value1" },
        { "Label": "Attribute2", "Value": "Value2" },
        { "Label": "Attribute3", "Value": "Amazon", "LinkType": "external", "Url": "https://www.amazon.com" }
    ],
    "Next": {
        "Label": "Go Home"
    },
    "Graphic": {
        "Include": true
    },
    "Heading": "I have updated your car rental reservation for pickup on July 22."
}
```
"SubHeading": "You will be receiving a confirmation shortly. Is there anything else I can help with today?",
}

Output Data Example

{
    "Action": "Next",
    "ViewResultData": {
        "Label": "Go Home"
    }
}

Cards view

The **Cards view** allows you to guide your agent by presenting them with a list of topics to choose from as soon as they accept the contact.

Interactive [documentation](#) for **Cards view**

*Present cards to your agents.* The following image shows an example of six cards that are presented to the agent: one to make a new reservation, and the others to review reservations for upcoming trips.

When agents choose a card, more info is revealed. The following image shows an open card that displays details for a reservation.
Sections

- It is list of objects with Summary and Detail. It must be provided to create Card and Detail.
- Consists of Summary and Detail. For more information see [Summary and Detail](#).

**AttributeBar (Optional)**

- Optional, if provided will display the Attribute bar at the top of the view.
- Is a list of objects with required properties, **Label**, **Value**, and optional properties **LinkType**, **ResourceId**, **Copyable** and **Url**. For more information, see [Attribute](#).
  - **LinkType** can be external or connect application such as case.
    - When it is *external*, a user can navigate to a new browser page, which is configured with **Url**.
    - When it is *case*, a user can navigate to a new case detail on the Agent workspace, which configured with Resourceld.
  - **Copyable** allows users to copy the Resourceld by choosing it with your input device.

**Heading (Optional)**
- String that displays as the page title

**Back (Optional)**

- It is an object or string with a Label which will control what is displayed in the link text. For more information, see [ActionProps](#).

**NoMatchFound (Optional)**

- It is a string that displays for a button that is below Cards. For more information see [ActionProps](#).

**Input Data Example**

```json
{
   "AttributeBar": [{
      "Label": "Queue",
      "Value": "Sales"
   },
   {
      "Label": "Case ID",
      "Value": "1234567"
   },
   {
      "Label": "Case",
      "Value": "New reservation"
   },
   {
      "Label": "Attribute 3",
      "Value": "Attribute"
   }
],
"Back": {
   "Label": "Back"
},
"Heading": "Customer may be contacting about...",
"Cards": [{
   "Summary": {
      "Id": "lost_luggage",
      "Icon": "plus",
```
"Heading": "Lost luggage claim",

"Detail": {
  "Heading": "Lost luggage claim",
  "Description": "Use this flow for customers that have lost their luggage and need to fill a claim in order to get reimbursement. This workflow usually takes 5-8 minutes",
  "Sections": {
  },
  "Actions": [
    "Start a new claim",
    "Something else"
  ]
},

{
  "Summary": {
    "Id": "car_rental",
    "Icon": "Car Side View",
    "Heading": "Car rental - New York",
    "Status": "Upcoming Sept 17, 2022"
  },
  "Detail": {
    "Heading": "Car rental - New York",
    "Sections": {
      "TemplateString": "<p>There is no additional information</p>"
    }
  }
},

{
  "Summary": {
    "Id": "trip_reservation",
    "Icon": "Suitcase",
    "Heading": "Trip to Mexico",
    "Status": "Upcoming Aug 15, 2022",
    "Description": "Flying from New York to Cancun, Mexico"
  },
  "Detail": {
    "Heading": "Trip to Mexico",
    "Sections": {
      "TemplateString": "<p>There is no additional information</p>"
"Summary": {
  "Id": "fligh_reservation",
  "Icon": "Airplane",
  "Heading": "Flight to France",
  "Status": "Upcoming Dec 5, 2022",
  "Description": "Flying from Miami to Paris, France"
},
"Detail": {
  "Heading": "Flight to France",
  "Sections": {
    "TemplateString": "<p>There is no additional information</p>"
  }
},
"Summary": {
  "Id": "flight_refund",
  "Icon": "Wallet Closed",
  "Heading": "Refund flight to Atlanta",
  "Status": "Refunded July 10, 2022"
},
"Detail": {
  "Heading": "Refund trip to Atlanta",
  "Sections": {
    "TemplateString": "<p>There is no additional information</p>"
  }
},
"Summary": {
  "Id": "book_experience",
  "Icon": "Hot Air Balloon",
  "Heading": "Book an experience",
  "Description": "Top experience for european travellers"
},
"Detail": {
  "Heading": "Book an experience",
  "Sections": {
    "TemplateString": "<p>There is no additional information</p>"
  }
}
Output Data Example

```
{
  Action: "ActionSelected",
  ViewResultData: {
    actionName: "Update the trip"
  }
}
```

### HTML and JSX support

You can customize the look and feel of the layouts of View resources by leveraging HTML or JSX when you pass in input parameters to the show view view block.

As a simple example, create a flow with one show view view block and select the **Details view**. In the **Sections** field use the below JSON to see how either HTML or JSX expressions get processed.

#### HTML example

```
{
  "TemplateString":
    "<TextContent>Steps:<ol><li>Customer provides incident information</li><li>Customer provides receipts and agrees with amount</li><li>Customer receives reimbursement</li></ol></TextContent>"
}
```

#### JSX example

```
{ "TemplateString":
    "<TextContent>Steps:<ol><li>Customer provides incident information</li><li>Customer provides receipts and agrees with amount</li><li>Customer receives reimbursement</li></ol></TextContent>"
}
No-code UI builder

You can create the view resources used in step-by-step guides by using Amazon Connect's no-code UI builder. With this feature, you are able to drag and drop UI components onto a canvas, arrange your layout, and edit the properties of each component. UI components are available on the left hand side of the screen and are grouped inside collapsible containers. The center of the screen is the canvas that shows you what your view resource looks like. The right hand side of the screen is where the properties are located.

UI component library

To learn more about all of the individual UI components and how to configure these components, see our interactive documentation.
UI component library
Containers

Containers are a core building block to make views. You are able to move UI components (including other containers) into a container in order to group them together logically and visually on the page. In order to keep the contents of the page relatively consistent as you customize the top level view settings, we highly encourage using containers in all of your views. Containers also come with column layout support, allowing you to organize the contents with a container.

Form

In order to create a form, you must use the form component. You can drag and drop the form component onto the canvas from the UI library or start off with the Form Example template that uses a form component. Effectively, the form component is a special type of container into which you are able to insert input fields and a submit button. When the submit button is pressed by the user interacting with a guide, the system will pass along all of the values entered into the form fields back to the contact flow. At that point, in the contact flow, you will be able to customize your own business logic and send/retrieve data to third-party systems using lambda flow blocks.
Customize panel

On the right hand side of the no-code UI builder is the **Customize** panel. In this panel you will be able to set a range of settings for your view including column layouts, colors, dynamic data mapping, sample data, and static data definitions. Both global settings for the entire view resource as well as local settings at the component level are configured in this panel.
Global settings

Global settings control the overall configuration of your view. To find global settings, navigate to the Customize panel on the right hand side of the screen and choose the globe icon, which is highlighted in the following image. Global Settings that exist today are layouts and colors. For more details on columns, see Layout columns. Alignment controls the relative location of components either to the left, center, or right of the view. There are three color fields available at the global level for the view resource: primary color, secondary color, and neutral color. Each component in the view will apply these settings by default. However, when customizing a component, you are able to override these global color settings.
Layout columns

The view resource uses a flexbox pattern with 12 columns. Instead of components being placed onto the canvas in a pixel perfect manner, components occupy a relative position to one another, allowing the view to responsively scale up and down in size without loosing the composition of the view. In the Global settings you able to determine how you want to group your columns.

For example, in the **Column** section, you can choose to divide the view into two sections of 6 columns and get the following layout.
You could also use the **Customize** slider to alter the ratios of these groupings. For example, you can set it so the left hand side of the view is 4 columns and the right hand side is 8.
### Enter Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>City</td>
<td>New York City</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>212-123-4567</td>
</tr>
<tr>
<td>Email Address</td>
<td>name@company</td>
</tr>
</tbody>
</table>

- **New Offers**
  - **Flight Deals**
    - Click here to learn more about the deals available
  - **Automobiles**
    - Click here to learn more about the deals available
  - **Bicycles**
    - Click here to learn more about the deals available
Dynamic fields

For some components, you won't know what values get populated until a guide is used at runtime. For example, if you are making a screen pop, you might know that you want to surface the customer's name and profile ID, but the values of these fields will change from contact to contact.

To set a specific field to have a component value, you can open up the properties tab for that component and select the check box *This is dynamic* that appears next to the field in question. The most common fields that requires dynamic values are the *Value* field for display fields and the *DefaultValue* field found in form inputs. Technically, any field both visible and hidden to an agent can be dynamically determined at runtime, which is why every field in the properties tab has a *This is dynamic* option that you may select.

As an example, we can take a look at the *AttributesBar* component.*This is dynamic*, the label of the display field found in the attributes bar, is statically defined as *Customer Name*, whereas the
actual value that populates this field is dynamic, and therefore will be determined by the data that gets passed in at runtime into the **Show view block**.

You also have the option to set all of the attributes of a component as dynamic. In this case, everything about this field, including the label, will be determined at runtime based on the values passed into the **Show view block**. In this case, **Customer Name** is now sample data that you can use to get a sense of what the agent will see when they use a guide, but this value is not viewable to the agent.
You can also set all of the sub-components of special containers as dynamic. For example, with the attributes bar, you can select the **This is dynamic** checkbox to make all of the attributes dynamic and therefore determined by whatever gets passed into the **Show view block** at runtime.
Attributes

- This is dynamic
  - Attributes-1
  - Attributes-2
  - Attributes-3

- This is dynamic
  - Label
    - This is dynamic
      - Active Case

- Value
  - This is dynamic
    - Attribute 2

- LinkType
  - This is dynamic
    - Case

- Url
  - This is dynamic
Setting actions that appear in flows

In order for a user to proceed to a new page when using guides, they will need to choose a button. When configuring buttons in the no-code UI builder, such as a submit form button, you will be able to determine an **Action** for this button. When a user chooses the button at runtime when using a guide and the response message is sent to flows, the **Action** value will determine which branching path will be followed. For example, if a view has three buttons on it, each with different actions, then those actions will appear on the show view block as different paths, allowing you to quickly configure the appropriate branching logic in flows.
Setting actions that appear in flows

Amazon Connect Administrator Guide

Action

NextPage
Saving and publishing view versions

View resources have versioning support that lets you audit and even re-use the previous iterations of a view you have created and/or used in step-by-step guides. After you make changes to your view, it is important to choose the **Save** button in order for the view resource to get updated. Once you are ready for a view to be used in a step-by-step guide contact flow, you can choose the **Publish** button. Only view versions that have been published will appear in the **Show view block** for use in a flow.

**Note**

In order to save a view, you must have entered a name for the view. You can set the name of the view in the top left hand corner of the no-code UI builder.

Templates to get started quickly

Included in the no-code UI builder are ready made templates you can use to pre-populate your canvas with components. By navigating to the **Templates** tab in the **Create** panel on the left hand side, you will be able to select one of the template options. Once the template appears on the canvas, you can add more components, delete components, and do any other type of configuration you can do with a view resource built from scratch.

If you have already placed UI components onto the canvas, these components will be overwritten and the template will take their place. These changes will only be finalized once you **Save** the view resource, so if you use a template in error, you can leave the page and come back to return to your last saved view resource version.
Templates to get started quickly
Sample data

Sample data can be used to see what your final view will look like to the user even when the actual data fields that will be displayed are dynamically determined at runtime. When **This is dynamic** is selected for a field, the value entered into the input box for that field is sample data that will appear in the canvas. This sample data is for view purposes only and will only appear in the Amazon Connect admin website.

For example, in the following image, **Address Line 1** in the **Mailing address** is a dynamic default value that will be populated at run-time by the address found in the customer profile. However, since the person building the view resource would like to see what the final UI will look like for their agent, they have entered a text default value. This value **7 W 34th St** is for display purposes only in the Amazon Connect admin website and will not appear to the agent.

![Form Example](image)

### How to invoke a guide at the start of a contact

After you've created your flows, you will be able to dynamically determine which ones to surface by setting the **DefaultFlowForAgentUI** event hook in your flows using the **Set event flow** block. As long as this event hook is set before a contact gets routed to a queue, the agent UI will show this flow after the agent accepts the contact.

For example, by checking the IVR responses, queue name, and customer info, you can create branching logic in flows that determines which flow ID to set. Use the **Check attribute** block to set your conditional logic and the **Set event flow** block to set the flow you want to send to your agent.
The following image shows the **Properties** page for the **Set event flow** block. **Event hook** is set to **Default flow for Agent UI**.

### Set event flow

Specify a flow to run when a contact event or interaction occurs, such as an agent accepting or disconnecting from a call or placing a customer on hold. **Info**

#### Select event

- **Select an event hook**
  - **Default flow for Agent UI**

#### Select a flow

- **Set manually**
- **Set dynamically**

---

How to invoke a guide at the start of a contact
Display contact attributes in the agent workspace

A simple use case of step-by-step guides is to surface contact attributes to your agents at the start of a contact in order to give them the context they need at the start of the contact so they can dive right into problem solving. This feature is sometimes referred to as a Screen Pop. To implement this use case, follow the example of how to deploy a Details view. For more information see View resource.

Disposition codes

A simple use case of step-by-step guides is to have an agent enter a disposition code at the end of the contact. To give your agents the ability to set disposition codes at the end of a contact or complete other post-call work, create a flow that has one Show view block and one Set contact attributes block.

- Use the Show view block to create a Form view that gives the agents the required input field.
- Use the Set contact attributes block to save the response as contact attributes.

In addition, you can also use an Invoke AWS Lambda function block to send the entered data to an external system.

After you've created your flow, you will be able to dynamically determine which one to surface at the end of a contact by setting the DisconnectFlowForAgentUI as a custom attribute in your contact flows. As long as this attribute is set before a contact ends, the agent UI will surface this form after a contact ends.

The following image shows the properties page for a Set contact attributes. It is configured to save the response in a user-defined attribute.
PII Redaction

By default, any information passed through a guide is included in the contact record transcript. To prevent PII from appearing in your contact record transcript, you will want to use the Set recording and analytics behavior block in your step-by-step guide contact flow, enable Contact Lens, and enable the redaction of sensitive date.

For full details on how to enable PII redaction, see Enable redaction of sensitive data.
Third-party applications (3p apps) in the agent workspace (Preview)

This is prerelease documentation for a service in preview release. It is subject to change.

Amazon Connect agent workspace is a single, intuitive application that provides your agents with the tools and step-by-step guidance they need to resolve issues efficiently, improve customer experiences, and onboard faster. For more information, see Customize the Amazon Connect Agent Workspace.

You have the option to use first-party applications, such as Customer Profiles, Cases, Amazon Q in Connect, and features such as step-by-step guides. With support for third-party applications, you can unite your contact center software, built by yourself or by partners in one place. For example, you can integrate your proprietary reservation system or a vendor-provided metrics dashboard, into the Amazon Connect agent workspace.

If you are a developer interested in building a third-party application, review the documentation here.

Contents

- Onboard third-party applications (Preview)
- Security profiles permissions for third-party applications (Preview)
- Access third-party applications in the agent workspace (Preview)
- Third-party application SSO Federation setup (Preview)

Onboard third-party applications (Preview)

This is prerelease documentation for a service in preview release. It is subject to change.

Requirements

If you're using custom IAM policies to manage access to third-party applications, your users need the following IAM permissions to integrate a third-party application using the AWS Console. In addition to AmazonConnect_FullAccess, users need:
How to integrate a third-party application

1. Open the Amazon Connect console (https://console.aws.amazon.com/connect/).

2. On the left navigation pane, choose Third-party applications. If you do not see this menu, it's because it is not available in your region. To check the regions where this feature is available, see Availability of Amazon Connect services by Region.

3. On the Third-party applications page, choose Add application.
4. On the Add application page, enter:

   a. Basic information

      i. **Display name**: A friendly name for the application. This name will display on security profiles and to your agents on the tab within the agent workspace. You may come back and change this name.

      ii. **Namespace**: The official name that is unique for your application. If you have only one application per access URL, we recommend that you use the origin of the access URL. You may not change this name.

      iii. **Description (optional)**: You may optionally provide any description for this application. This description will not display to agents.

   b. Access

      i. **Access URL**: This is the URL where your application is hosted. The URL must be secure, starting with https, unless it's a local host.

      **Note**

      Not all URLs can be iframed. Here are two ways to check if the URL can be iframed:
i. There is a third-party tool available to help check if a URL can be iframed that is called Iframe Tester.

A. If a URL can be iframed, it will render in a preview on this page.
B. If a URL cannot be iframed, it will display an error in the preview on this page.

- It is possible that this website displays an error, and the app can still be iframed in the agent workspace. This is because the app developer can lock down their app to only be embeddable into the workspace and nowhere else. If you received this app from an app developer, we recommend that you still try integrating this app into the agent workspace.

ii. For technical users: Check the security policy content of the application you are trying to integrate.

A. Firefox: Hamburger menu > More tools > Web developer tools > Network
B. Chrome: 3 dots menu > More tools > Developer tools > Network
C. Other browsers: Locate the network settings in the developer tools.
D. The Content-Security-Policy frame-ancestors directive should be https://your-instance.my.connect.aws.

- If the directive is same origin or deny, then this URL cannot be iframed by AWS/Amazon Connect

Here’s what you can do if the app cannot be iframed:

- If you control the app/URL, you can update the app’s content security policy. Follow the best practices for app developers/ Ensuring that apps can only be embedded in the Connect agent workspace section here.
- If you do not control the app/URL, you can try reaching out to the app developer and asking them to update the app’s content security policy.
ii. **Approved origins (optional):** Allowlist URLs that should be permitted, if different than the access URL. The URL must be secure, starting with https, unless it's a local host.

c. **Instance association**

i. You may give any instance(s) within this account-region access to this application.

ii. While associating the application to an instance is optional, you will not be able to use this application until you associate it with instance(s).

5. **Choose Add application.**

- You will be limited by quotas for the number of applications you can add. For more information, see the Application per region quota.

6. If the application was successfully created, you will be returned to the Third-party applications page, you will see a success banner, and you should see the application on the list.

- If there was an error in either creating the application or associating the application to an instance, then you will see an error message, and you can take the corresponding action to correct the issue.
Security profiles permissions for third-party applications (Preview)

This is prerelease documentation for a service in preview release. It is subject to change.

This topic describes the security profiles permissions that are required to access third-party applications that you have onboarded and associated. For a list of third-party application permissions and their API name, see List of security profile permissions.

Third-party application permissions

Note
After associating an application to an instance, you may have to wait up to 10 minutes to see the application appear the security profiles Agent Applications menu.

Any applications that you have onboarded to AWS and associated with your Amazon Connect instance will appear on the security profiles Agent Applications menu, as in the following image:

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>Access</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wisdom</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Custom views</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Maps</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Notes</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Note
You will also need to give access to the CCP in order for the app launcher menu to appear.
Contact Control Panel (CCP)
This allows various levels of access to the Call Control Panel (CCP).

<table>
<thead>
<tr>
<th>Type</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Contact Control Panel</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Once you have given permissions, you can review how to [Access third-party applications in the agent workspace (Preview)](#).

**Access third-party applications in the agent workspace (Preview)**

This is prerelease documentation for a service in preview release. It is subject to change.

**Note**

The admin must have [integrated the application](#) and the agent must have [access to the application](#) by using security profiles. The agent must also have access to the CCP in order for the application launcher to appear.

To access the agent workspace, go to the following URL:

https://instance name.my.connect.aws/agent-app-v2/

From the agent workspace, agents can access third-party applications in the agent workspace by using the app launcher. Ensure that agents have permissions to:

- Access the CCP
- Access to at least one third-party applications

Agents will then see a menu in the top-right corner of the agent workspace called the app launcher. The app launcher will show a list of applications that the agent has access to. The agent
can launch applications in the idle state (when they have no contacts) or when they are on a contact (call, chat, or task). Once an app is opened for a given contact, then it will stay open until that contact is closed.

Notes app

Map app
Third-party application SSO Federation setup (Preview)

*This is prerelease documentation for a service in preview release. It is subject to change.*

A user can use Single-Sign-On to federate into multiple third-party applications that have been setup within their Amazon Connect instance without the need to authenticate separately for each application.

**Setup SSO for third-party apps that exist within your Amazon Connect instances**

1. Setup an Identity Provider or use an existing Identity Provider.
2. Setup users within the Identity Provider.
3. Setup a Connect instance and [Configure SAML with IAM for Amazon Connect](#).
4. Setup other applications within your Identity Provider which you will be integrating with your Connect instance.
5. Attach each individual user identity to any applications within the Identity Provider that will be integrated with your Connect instance. You can control which agent has access to an application on the connect agent workspace by providing more granular application specific
permissions in security profiles. For more information, see Security profiles permissions for third-party applications (Preview).

6. Once a user has signed into their Identity Provider, they can federate into their Connect instance which has Third-party applications configured and they can federate into each application (if the application has been setup for SSO) without the need of their username and password.
Use Amazon Q in Connect for generative AI–powered agent assistance in real-time

Note

**Powered by Amazon Bedrock**: AWS implements [automated abuse detection](https://aws.amazon.com/bedrock/). Because Amazon Q in Connect is built on Amazon Bedrock, users can take full advantage of the controls implemented in Amazon Bedrock to enforce safety, security, and the responsible use of artificial intelligence (AI).

Amazon Q in Connect is a generative AI customer service assistant. It is an LLM-enhanced evolution of Amazon Connect Wisdom that delivers real-time recommendations to help contact center agents resolve customer issues quickly and accurately.

Amazon Q in Connect automatically detects customer intent during calls and chats using conversational analytics and natural language understanding (NLU). It then provides agents with immediate, real-time generative responses and suggested actions. It also provides links to relevant documents and articles.

In addition to receiving automatic recommendations, agents can also query Amazon Q directly using natural language or keywords to answer customer requests. Amazon Q works right within the Amazon Connect agent workspace.

Amazon Q in Connect is available by API to be used in an existing agent workspace. For more information, see the [Amazon Q in Connect API Reference Guide](https://docs.aws.amazon.com/connect/latest/api/API_AutoRecommendationList.html).

Note

To use Amazon Q in Connect with calls, you must enable Amazon Connect Contact Lens. Contact Lens is not required to use Amazon Q in Connect with chats.

Currently, Amazon Q in Connect can be used in compliance with [GDPR](https://ec.europa.eu/info/law/law-topic/data-protection-reform_en) and is pending additional certifications held by Amazon Connect.

The following image shows how an article may appear in the agent application when the agent is on a call.
1. The agent is on a call.
2. The agent can ask natural-language questions.
3. Amazon Q in Connect provides a response that the agent can share directly with the customer. For example, they can copy and paste the response into a chat, or read it over the call.
4. Amazon Q in Connect provides more information for the agent, for example, a summary of the solution or of the next steps they should take.
5. Amazon Q in Connect provides links to specific articles.

Enable Amazon Q in Connect for your instance

There are two ways you can enable Amazon Q in Connect for your instance:

- Use the Amazon Connect console. There are instructions on this page.
- Use the Amazon Q in Connect API to ingest content.

The APIs support the ingestion of HTML, Word, PDF, and text.

- Plain text files must be in UTF-8.
- Word documents must be in DOCX format.
• Word documents are automatically converted to a simplified HTML view and will not retain the source document's font family, size, color, highlighting, alignment, or other formatting features such as background colors, headers or footers.

• PDF files cannot be encrypted or password protected.

• Actions and scripts embedded into PDF files are not supported.

Following is an overview of the steps to enable Amazon Q in Connect:

1. Create an Amazon Q in Connect Assistant (domain). An Assistant is made up of one knowledge base.

2. Create an encryption key to encrypt the excerpt that is provided in the recommendations to the agent.

3. Create a knowledge base using external data:
   • Add data integrations from Amazon S3, Microsoft SharePoint Online, Salesforce, ServiceNow, and ZenDesk using prebuilt connectors in the Amazon Connect console.
   • Encrypt the content importing from these applications using a KMS key.
   • Specify the sync frequency.

**Before you begin**

Following is an overview of key concepts and the information that you'll be prompted for during the setup process.

**About the Amazon Q in Connect domain**

When you enable Amazon Q in Connect, you create an Amazon Q in Connect domain: an Assistant that is made up of one knowledge base. Following are guidelines for creating Amazon Q in Connect domains:

• You can create multiple domains, but they don't share external application integrations or customer data between each other.

• Each domain can be associated with one or more Amazon Connect instances, but each Amazon Connect instance can be associated with only one domain.

• All the external application integrations you create are at a domain level. All of the Amazon Connect instances associated with a domain inherit the domain's integrations.
You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain.

**How do you want to name your Amazon Q in Connect domain?**

When you enable Amazon Q in Connect, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, *ExampleCorp*.

**Create AWS KMS keys to encrypt the domain and the connection**

When you enable Amazon Q in Connect, by default the domain and connection are encrypted with an AWS owned key. However, you have the option to create or provide two AWS KMS keys:

1. One for the Amazon Q in Connect domain, used to encrypt the excerpt provided in the recommendations.
2. Another to encrypt the content imported from Amazon S3, Microsoft SharePoint Online, Salesforce, ServiceNow, and ZenDesk. Note that Amazon Q in Connect search indices are always encrypted at rest using an AWS owned key.

Step-by-step instructions for creating these KMS keys are provided in [Step 1: Add integration](#).

Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

If you choose to set up a KMS key where someone else is the administrator, the key must have a policy that allows `kms:CreateGrant`, `kms:DescribeKey`, and `kms:Decrypt` and `kms:GenerateDataKey*` permissions to the IAM identity using the key to invoke Amazon Q in Connect. To use Amazon Q in Connect with chat, the key policy for your Amazon Q in Connect domain must allow `kms:Decrypt`, `kms:GenerateDataKey*`, and `kms:DescribeKey` permissions to the `connect.amazonaws.com` service principal.

For information about how to change a key policy, see [Changing a key policy](#) in the AWS Key Management Service Developer Guide.

**Step 1: Add integration**

Following are instructions for how to create a new domain and add an integration.

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

![Amazon Connect instances page](image)

3. In the navigation pane, choose **Amazon Q in Connect**, and then choose **Add domain**.

4. On the **Add domain** page, choose **Create a domain**.

5. In the **Domain name** box, enter a friendly name that's meaningful to you, such as your organization name, for example, **ExampleCorp**.

6. Under **Encryption**, create or enter your own AWS KMS key for encrypting your Amazon Q in Connect domain. Following are the steps to create your KMS key:

   1. On the **Add domain** page, choose **Create an AWS KMS key**.

   2. A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.

   ![Configure key page](image)

   3. On the **Add labels** page, add a name and description for the KMS key, and then choose **Next**.

   ![Add labels page](image)
4. On the **Define key administrative permissions** page, choose **Next**.

5. On the **Define key usage permissions** page, choose **Next**.

6. On the **Review and edit key policy** page, scroll down to **Key policy**. To use Amazon Q in Connect with chat, modify the key policy to allow the `kms:Decrypt`, `kms:GenerateDataKey*`, and `kms:DescribeKey` permissions to the `connect.amazonaws.com` service principal. The following code shows a sample policy.

```json
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iamp:your_accountId:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "connect.amazonaws.com"
            },
            "Action": ["kms:Decrypt",
                        "kms:GenerateDataKey*",
                        "kms:DescribeKey"
            ]
        }
    ]
}
```
Next, choose Finish.

In the following example, the name of the KMS key starts with bcb6fdd:

7. Return to the tab in your browser for the Amazon Connect console, Amazon Q in Connect page. Click or tap in the AWS KMS key for the key you created to appear in a dropdown list. Choose the key you created.

7. Choose Add domain.

8. On the Amazon Q in Connect page, choose Add integration.

9. On the Add integration page, choose Create a new integration, and then select the source.

10. In the Integration name box, assign a friendly name to the integration, one that is meaningful to you.

Tip

If you are going to have multiple integrations from the same source, we recommend you develop a naming convention to make them easy to distinguish.

11. Under Connection with [Source], choose Create a new connection, and then enter a friendly name for the connection that is meaningful to you.

12. Enter the instance URL of the source you want to connect to, and then choose Log in to [Source].

13. Under Encryption, choose Create an AWS KMS key. This key encrypts the connection to the external application that stores content. Following are the steps to create your KMS key:
1. On the Add domain page, choose Create an AWS KMS key.

2. A new tab in your browser opens for the Key Management Service (KMS) console. On the Configure key page, choose Symmetric, and then choose Next.

3. On the Add labels page, add a name and description for the KMS key, and then choose Next.

4. On the Define key administrative permissions page, choose Next.

5. On the Define key usage permissions page, choose Next.


   In the following example, the name of the KMS key starts with bcb6fdd:
7. Return to the tab in your browser for the Amazon Connect console, Amazon Q in Connect page. Click or tap in the AWS KMS key for the key you created to appear in a dropdown list. Choose the key you created.

14. Under Ingestion start date, choose when you want Amazon Q in Connect to import records from your application, and how often.

1. Ingest all records defaults to the earliest date possible.

15. Under Sync frequency, the default is hourly. You can use the dropdown to choose Every 3 hours or Daily. On-demand syncing is not available.
Step 2: Select object and fields

In this step you choose the object and fields from the source that you want to make available to your agents in Amazon Q in Connect.

1. In the **Available objects** dropdown menu, choose the object you want. Only knowledge objects appear in the menu.
2. Under **Select Fields for [object name]**, choose the fields you want to include. You'll notice that some fields, such as **AccountID** and **ID**, are already selected by default. These fields are required.

![Select Fields for [object name]](image)

3. Choose **Next**.

**Step 3: Review and integrate**

1. Review all the integration details.
2. Choose **Add integration**.

3. The integration is added to your list, as shown in the following example.

4. After an integration is created, you can edit the URI, but no other information.

**Step 4: Configure your flow for Amazon Q in Connect**

1. Add a **Amazon Q in Connect** block to your flow. The block associates an Amazon Q in Connect domain to the current contact. This enables you to display information from a specific domain, based on criteria about the contact.
To use Amazon Q in Connect with calls, you must enable Amazon Connect Contact Lens in the flow by adding a Set recording and analytics behavior block that is configured for Contact Lens real-time. It doesn't matter where in the flow you add the Set recording and analytics behavior block.

**Note**

Contact Lens is not required to use Amazon Q in Connect with chats. Amazon Q in Connect, along with Contact Lens real-time analytics, is used to recommend content that is related to customer issues detected during the current call.

**When was your knowledge base last updated?**

To confirm the last date and time that your knowledge base was updated (meaning a change in the content available), use the GetKnowledgeBase API to reference lastContentModificationTime.

**Security profile permissions for Amazon Q in Connect**

Assign the following Agent Applications permission to the agent's security profile:

- **Amazon Q - Access**: Enables agents to search for and view content. They can also receive automatic recommendations during calls if Contact Lens is enabled. Contact Lens is not required to use Amazon Q with chats.

For information about how to add more permissions to an existing security profile, see Update security profiles.

By default, the Admin security profile already has permissions to perform all Amazon Q activities.

**Access Amazon Q in Connect in the agent application**

If you're using the CCP that is provided with Amazon Connect, after you enable Amazon Q in Connect, share the following URL with your agents so they can access it:

- https://instance name.my.connect.aws/agent-app-v2/
If you access your instance using the `awsapps.com` domain, use the following URL:

- `https://instance name.awsapps.com/connect/agent-app-v2/`

For help finding your instance name, see [Find your Amazon Connect instance name](#).

By using the new URL, your agents can view the CCP and Amazon Q in Connect in the same browser window.

If CCP is embedded in your agent's application, see [Initialization for CCP, Customer Profiles, and Amazon Q in Connect](#) in the *Amazon Connect Streams Documentation* for information about how to include Amazon Q in Connect.

For more information about the agent's experience using Amazon Q in Connect, see [Search for content using Amazon Q in Connect](#).
Amazon Connect Cases

Amazon Connect Cases enables your customer service organization to track, collaborate, and resolve customer cases.

A case represents a customer's issue. It is created to record the customer's issue, the steps and interactions taken to resolve the customer's issue, and the outcome.

Without doing any integration work, you can enable Cases for your contact center. You can set up cases to be created when contacts come in, and collect information from the customer to display on the case. Alternatively, agents can manually create cases. When an agent accepts a contact, they have context about an issue and can immediately start solving it. You can create tasks to track and route follow up steps to resolve the case.

The following image shows an example case as it appears in the agent application.

Getting started with Cases

We recommend reviewing these topics to help you get started:

- Enable Cases
- Assign permissions
- Create case fields and case templates
Enable Cases

This topic explains how to enable Amazon Connect Cases using the Amazon Connect console. To use the API, see Amazon Connect Cases API Reference.

**Tip**

A case is always associated with a customer profile. You must have Customer Profiles enabled. Check your instance settings in the Amazon Connect console, and if a Customer Profiles domain does not yet exist, see Enable Customer Profiles for your instance.

Requirements

If you're using custom IAM policies to manage access to the Amazon Connect Cases, your users need the following IAM permissions to onboard to Cases using the Amazon Connect console:

- connect:ListInstances
- ds:DescribeDirectories
- connect:ListIntegrationAssociations
- cases:GetDomain
- cases:CreateDomain
- connect:CreateIntegrationAssociation
- connect:DescribeInstance
- iam:PutRolePolicy

For more information, see Required permissions for using custom IAM policies to manage Cases.
How to enable Amazon Connect Cases

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. On the left navigation menu, choose Cases. If you don't see this option, it may not be available in your Region. For information about where Cases is available, see Cases availability by Region.

4. Choose Enable cases to get started.

5. On the Cases page, choose Add domain.

6. On the Add domain page, enter a unique, friendly name that's meaningful to you, such as your organization name.

7. Choose Add domain. The domain is created.

   If the domain is not created, choose Try again. If that doesn't work, contact AWS Support.

Next steps

After your cases domain is created, do the following:

1. Assign security profile permissions to agents and call center managers.

2. Create case fields. Fields are the building blocks of your case templates.

3. Create case templates. Case templates are forms that agents complete and reference in the agent application. Templates ensure the right information is collected and referenced for different types of customer issues.
4. Optionally, enable attachments across your Amazon Connect instance. This step allows your agents to upload files to cases.

5. Optionally, add the Cases block to your flows. This block enables you to get, update, or create cases automatically.

6. Optionally, set up case event streams to get near real-time updates when cases are created or modified.

Security profile permissions for Cases

This topic describes the security profiles permissions that are required to access and use Amazon Connect Cases. For a list of Cases permissions and their API name, see List of security profile permissions.

Required Cases permissions

The following image shows the security permissions used to manage access to Amazon Connect Cases functionality:

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cases</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Case Fields</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Case Templates</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Required Customer Profiles permissions

To use Amazon Connect Cases, your users also need permissions to Customer Profiles permissions, as shown in the following image.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Create</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer profiles</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Required queue, quick connect, and user view permissions

To be able to assign case ownership to users or queues, agents need permissions to view queues, quick connects, and users. To be able to view the author name on comments, agents need permission to view users. These permissions are shown in the following two images.

### Description of Cases permissions

- **Cases**: Manage who can access cases by using the agent application.

  - **View case**: Allows the user to view and search cases in the agent application. This includes viewing case data (for example, status, title, summary), contact history (for example, calls, chats, tasks with information such as start time, end time, duration, etc.), and comments.

  - **Edit case**: Allows the user to edit cases, which includes editing case data (for example, update case status), add comments, and associate contacts to cases.

  - **Create case**: Allows the user to create new cases, and associate contacts to cases.
• **Case Fields**: Manage who can configure case fields by using the Amazon Connect console.
  - **View Case Fields**: Allows users to view the case fields page and all of the existing case fields (could be system or custom).
  - **Edit Case Fields**: Allows users to edit any of the case fields (for example, change title, description, single-select options).
  - **Create Case Fields**: Allows users to create new case fields.

• **Case Templates**: Manage who can configure case templates by using the Amazon Connect console.
  - **View Case Fields**: Allows users to view the case fields page and all of the existing case fields (could be system or custom).
  - **Edit Case Fields**: Allows users to edit any of the case fields (for example, change title, description, single-select options).
  - **Create Case Fields**: Allows users to create new case fields.

When users have permissions to **View Case Fields** and **View Case Templates**, they will see the **Case fields** and **Case templates** options in their left navigation menu, as shown in the following image:
Required permissions for using custom IAM policies to manage Cases

If you're using custom IAM policies to manage access to the Amazon Connect Cases, your users need some or all of the permissions listed in this article, depending on the tasks they need to do.

View Cases domain details

There are two options for granting users IAM permissions to view Cases domain details on the Amazon Connect console.

Option 1: Minimum required IAM permissions

To view Cases domain details in the Amazon Connect console, users must have the following IAM permissions:

- connect:ListInstances
- ds:DescribeDirectories
- connect:ListIntegrationAssociations
- cases:GetDomain

Following is a sample IAM policy with these permissions:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsViewingConnectConsole",
            "Effect": "Allow",
            "Action": [
                "connect:ListInstances",
                "ds:DescribeDirectories"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIntegrationAssociations",
            "Effect": "Allow",
            "Action": "connect:ListIntegrationAssociations"
        }
    ]
}
```
Note the following:

- `cases:GetDomain` Action is required on Resource `*`
- `connect:ListIntegrationAssociations` action supports the instance resource type. See the table in [Actions defined by Amazon Connect](#).

**Option 2: Update the existing Amazon Connect policy with `cases:GetDomain` and `profile:SearchProfiles`**

Include the [AmazonConnectReadOnlyAccess](#) policy, and add `cases:GetDomain`, as shown in the following example.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "CasesGetDomain",
         "Effect": "Allow",
         "Action": [
            "cases:GetDomain"
         ],
         "Resource": "*"
      }
   ]
}
```
Onboard to Cases

There are two options for granting users IAM permissions to onboard to Cases using the Amazon Connect console.

Option 1: Minimum required permissions

To onboard to Cases by using the Amazon Connect console, users must have the following IAM permissions:

- `connect:ListInstances`
- `ds:DescribeDirectories`
- `connect:ListIntegrationAssociations`
- `cases:GetDomain`
- `cases:CreateDomain`
- `connect:CreateIntegrationAssociation`
- `connect:DescribeInstance`
- `iam:PutRolePolicy`
- `profile:SearchProfiles`

Following is a sample IAM policy with these permissions:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsViewingConnectConsole",
            "Effect": "Allow",
            "Action": [
                "connect:ListInstances",
                "ds:DescribeDirectories"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIntegrationAssociations",
            "Effect": "Allow",
            "Action": [
                "connect:ListIntegrationAssociations"
            ],
            "Resource": "*"
        }
    ]
}
```
Onboard to Cases

1. Create a new domain

   - Role: AWS Service Role for Amazon Connect
   - Permissions:
     ```json
     { "Resource": "*" },
     { "Sid": "CasesGetDomain",
       "Effect": "Allow",
       "Action": [ "cases:GetDomain" ],
       "Resource": "*" },
     { "Sid": "CasesCreateDomain",
       "Effect": "Allow",
       "Action": [ "cases:CreateDomain" ],
       "Resource": "*" },
     { "Sid": "CreateIntegrationAssociationsAndDependencies",
       "Effect": "Allow",
       "Action": [ "connect:CreateIntegrationAssociation",
                   "connect:DescribeInstance" ],
       "Resource": "*" },
     { "Sid": "AttachAnyPolicyToAmazonConnectRole",
       "Effect": "Allow",
       "Action": "iam:PutRolePolicy",
       "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect" },
     { "Sid": "ProfileSearchProfiles",
       "Effect": "Allow",
       "Action": [ "profile:SearchProfiles" ],
       "Resource": "*" }
     ]
     ```
Note the following:

- `cases:GetDomain` Action is required on Resource *
- You can scope the permissions to specific Amazon Connect tasks by using the information in [Actions, resources, and condition keys for Amazon Connect](#).
- `profile:SearchProfiles` Action is required because the `CreateCase` API calls the `SearchProfiles` API to search for customer profiles to validate against, and then associate the profile with the case.

**Option 2: Use a combination of existing policies**

The following combination of policies will also work:

- [AmazonConnect_FullAccess](#) policy
- [iam:PutRolePolicy](#) to modify the service-linked role. For an example, see [AmazonConnect_FullAccess policy](#).
- The following IAM policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CasesGetDomain",
      "Effect": "Allow",
      "Action": [
        "cases:GetDomain",
        "cases:CreateDomain"
      ],
      "Resource": "*
    },
    {
      "Sid": "ProfileSearchProfiles",
      "Effect": "Allow",
      "Action": [
        "profile:SearchProfiles"
      ],
      "Resource": "*
    }
  ]
}
```
Create case fields

Case fields are the building blocks for case templates. You create all of the possible fields of information (for example, VIN number, policy number, make/model of car) that you want agents to collect for a given customer issue.

After you create case fields, you can create case templates.

There are two types of case fields:

- **System case fields**: Amazon Connect provides system fields. You cannot change the name or description.
- **Custom case fields**: You can create custom case fields that are specific for your business. You must name the case field, and optionally provide a description. Note that the description appears only in the Amazon Connect console. It doesn't appear to agents.

How to create case fields

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create fields. For a list of required permissions, see Security profile permissions for Cases.
2. Verify the quota for case fields and request an increase if needed. For more information, see Amazon Connect Cases service quotas.
3. On the left navigation menu, choose Agent applications, Case fields.
4. The first time you create new fields, you'll notice several system fields are already present. You cannot change the name of these fields, but in some cases you can edit them.

   For example, Case Id is a system field. When a case is created, Amazon Connect adds a case ID automatically, and you cannot change it. Case reason is also a system field but you can edit it and enter reasons that are specific to your contact center.

5. Choose + New field.
6. Select the type of field you want to create. For example, you might choose Text if you want agents to be able to enter free form notes.
7. Assign a name to the field. It will appear to agents in the agent application.

8. Optionally, provide a description. It will only appear to admins on the Amazon Connect console. It does not appear to agents in the agent application.

9. Choose Save.

10. When you're done adding fields, you're ready to create a template.

**System case fields**

Amazon Connect provides system fields. You cannot change the name or description of a system field.

The following table lists the system case fields:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field ID (how you call the field in the API)</th>
<th>Field type</th>
<th>Description</th>
<th>Where the data comes from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned queue</td>
<td>assigned_queue</td>
<td>text</td>
<td>The Amazon Connect queue that is assigned to a case</td>
<td>Agent</td>
</tr>
<tr>
<td>Assigned user</td>
<td>assigned_user</td>
<td>text</td>
<td>The Amazon Connect user who is assigned to a case</td>
<td>Agent</td>
</tr>
<tr>
<td>Case ID</td>
<td>case_id</td>
<td>text</td>
<td>Unique Identifier of the case in UUID format (for example, 689b0beaa29-4340-896d-4ca3ce9b6226)</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Field name</td>
<td>Field ID (how you call the field in the API)</td>
<td>Field type</td>
<td>Description</td>
<td>Where the data comes from</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Case ID</td>
<td>case_id</td>
<td>text</td>
<td>Unique Identifier of the case in UUID format (for example, 689b0bea-aa29-4340-896d-4ca3ce9b6226)</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Case Reason</td>
<td>case_reason</td>
<td>single-select</td>
<td>The reason for opening the case</td>
<td>Agent</td>
</tr>
<tr>
<td>Customer</td>
<td>customer_id</td>
<td>text</td>
<td>The full ARN of the customer profile identified for the case is required when using the API. On the <strong>Cases: Fields</strong> page, the customer's name is displayed.</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Field name</td>
<td>Field ID (how you call the field in the API)</td>
<td>Field type</td>
<td>Description</td>
<td>Where the data comes from</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Date/Time Closed</td>
<td>last_closed_datetime</td>
<td>date-time</td>
<td>The date and time the case was last closed. It does not guarantee that a case is closed. If a case is reopened, this field contains the date/time stamp of the last time the status was changed to closed.</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Date/Time Opened</td>
<td>created_datetime</td>
<td>date-time</td>
<td>The date and time the case was opened.</td>
<td>Amazon Connect</td>
</tr>
<tr>
<td>Date/Time Updated</td>
<td>last_updated_datetime</td>
<td>date-time</td>
<td>The date and time the case was last updated.</td>
<td>Amazon Connect</td>
</tr>
</tbody>
</table>
### Custom case fields

You can create custom case fields that are specific for your business. You must name the case field, and optionally provide a description. Note that the description appears only in the Amazon Connect console. It doesn't appear to agents.

You can create fields that are type: number, text, single-select, or true/false.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field ID (how you call the field in the API)</th>
<th>Field type</th>
<th>Description</th>
<th>Where the data comes from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference number</td>
<td>reference_number</td>
<td>text</td>
<td>A friendly number for the case in 8-digit numeric format. Reference numbers (unlike the Case ID) are not guaranteed to be unique. We recommend that you identify the customer and then collect the reference number to correctly find the right case.</td>
<td>Agent</td>
</tr>
<tr>
<td>Status</td>
<td>status</td>
<td>single-select</td>
<td>Current status of the case</td>
<td>Agent</td>
</tr>
<tr>
<td>Summary</td>
<td>summary</td>
<td>text</td>
<td>Summary of the case</td>
<td>Agent</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>text</td>
<td>Title of the case</td>
<td>Agent</td>
</tr>
</tbody>
</table>
Single-select fields

For single-select case fields, whether system or custom, you can add value options that the field can take. For example, you can add options to the single-select system field Case reason such as General inquiry, Billing issue, or Product defect, that reflect the types of issues in your contact center.

About the Status field

You can add options to the single-select Status field, such as Investigating or Escalated to manager. The field comes with two options, Open and Closed, which cannot be changed.

Active/inactive field options

Single-select case fields can be active or inactive.
• **Active**: If a field option is active, it means that the field can be given that option. For example, based on the following image, the Status field can be set to **Closed**, **Open**, or **Pending**, as these are the only active options.

• **Inactive**: If you make the **Pending** option inactive, then the field can no longer be given that option. Any existing cases remain unchanged and can still have the status as **Pending**.

Single-select options have two parts:

1. Option name (shown to agents): The label that is displayed to agents in the agent application.
2. Option value (internal reference): The data that's collected. For example, for AWS Region, you may want to display **US West (Oregon)** but collect the data as **PDX**.

Field options appear to the agent in alphabetical order.

![Option value table](image)

**Create case templates**

*Case templates* are forms that ensure agents collect and reference the right information for different types of customer issues. For example, you can create a case template for vehicle damage issues, and require agents complete certain fields when they talk to a customer filing an insurance claim.

When you create a case template, you choose the name that appears to agents, the fields on the form, and the order of the fields.

⚠️ **Important**

Cases are always created based on a template.
How case templates look in the agent application

In the agent application, the agent sees the case fields in a Z-formation: case fields are displayed in two columns from left to right, top to bottom.

When you're building a case template, think of the information in the agent application as being divided into two sections where case fields are displayed to the agent:

- Top fields: This section is always visible on the case, even when agent is viewing sub-sections of the case (for example, Activity Feed or Comments).
More information: This is a tabbed subsection of the case. It is visible when agent is viewing another subsection, such as Activity Feed or Comments.

When you create and edit a template, you can do the following in each section:

- Change the order of the fields.
- Indicate if fields are required.

Some system fields, such as Title and Status, appear on all cases and are required. Other system fields, such as Customer, Summary, and Reference number, appear by default on the case details page. You can remove or rearrange these fields.

Each case that is created is connected to a customer profile from your Amazon Connect instance. On new case templates, the customer name appears by default on the case details page. You can remove or rearrange this field from your templates from the Amazon Connect console.

How to create a template

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create templates. For a list of required permissions, see Security profile permissions for Cases.
2. Verify the quota for case templates and request an increase if needed. For more information, see Amazon Connect Cases service quotas.
3. Verify the case fields you want to add to your case template have already been created.
4. On the left navigation menu, choose Agent applications, Case templates.
6. Assign a name to the template. It will appear to agents in the agent application. The following image shows an example of how templates appear, by default in alphabetical order:
7. In the **Top fields** section, you'll see some system fields already there. Choose **Add fields**, and use the dropdown to choose the field. Fields that are gray-out are already a part of the template. If you want agents to complete the field in order to save the form, choose **Required**.

8. In the **More information** section, choose the fields you want to appear.

9. When you're done, choose **Save**. The template is immediately made available to agents in the agent application.

### Case layouts

This topic is intended for developers who are using the Amazon Connect Cases APIs.

There is an underlying resource called a *case layout* that is linked to the case template. Technically, it is the case layout that holds the display elements for a case, such as:

- Which fields to display.
- The section, either Top panel or More information.
- The order within a section to display these fields

Whereas it's the case template that mandates a particular schema, such as required case fields.

The case layout is linked to a case template.
Note
You can create a case template and not link it to a case layout. Any case created with a case template that is not linked to a case layout will display system fields in a default order.

Set up case assignment

To help your organization clearly track ownership of cases and resolve them faster, you can ensure every case has an assigned owner who is responsible for case resolution. The owner can be a queue or an individual user.

Note
Assigning a case owner does not route the case to the queue or the individual.

The following image shows the Case list view in the agent workspace. You can filter by unassigned cases, for example, and assign ownership as needed. The default view is set to cases assigned to the agent who is viewing the list.

Contents

- Set up agents and flows case assignment
Set up agents and flows case assignment

To enable case assignment in your Amazon Connect instance, configure the following resources:

1. **Case template.** Add the following *system case fields* to a new or existing case template:
   - Assigned queue
   - Assigned user

2. To enable agents to assign case ownership in the agent workspace:
   - **Security profile.** Grant agents permission to view the queues, users, and quick connects that are going to appear in the dropdown lists in the agent workspace. For more information, see [Required queue, quick connect, and user view permissions](#).
   - **Quick connects.** Create user and queue quick connects for each user and queue that you want to appear in the dropdown lists. For instructions, see [Create quick connects](#).
   - **Queues.** Add the quick connects to the agent's queue. For instructions, see [Create a queue](#).
   - **Routing profile.** Add the queue to the agent's routing profile. For instructions, see [Create a routing profile](#).

   Agents see only those quick connects that are added to the queues assigned to their routing profile.

3. To configure the Cases block to assign case ownership automatically during a flow, set the **Request Fields** section to **Assigned Queue** or **Assigned User**. For an image and more instructions, see [How to configure the Cases block to assign case ownership in a flow](#).

How agents assign case ownership

The following image shows the agent workspace. Agents choose the **Assign to** dropdown box to assign ownership of a case to themselves (the default option), a queue, or another user.
If agents assign ownership of a case to a queue or another user, they are presented with a prompt to choose from a filtered list of queues or users. The filtered list of available queues or users is based on the quick connects in the agent's routing profile.

**Assign to queue**

The following image shows an example dropdown list of queues in the agent workspace. For this list of queues to be displayed to an agent: create a quick connect for each queue, and then add the queue to the agent's routing profile.
Assign to user

The following image shows an example dropdown list of users in the agent workspace. For this list of users to be displayed to an agent: create a quick connect for each user, assign the quick connects to the queue, add the queue to the agent's routing profile.

A quick connect must exist for each **queue** that appears in the list.

A quick connect must exist for each **user** that appears in the list.
How to configure the Cases block to assign case ownership in a flow

You can configure the Cases block to automatically populate the Assigned queue or Assigned user ownership fields. When agents view the case in the agent workspace, the case ownership is already set. Agents can override the assignment as needed, but are restricted to the queues and users that are available in their routing profile.

The following image shows an example of the Properties page for the Cases block. The Request Fields section is configured to Set manually, Assigned queue. You must enter the full ARN of the queue.
There are situations where you may want to set the assigned queue or assigned user dynamically. For example, when the customer enters a DTMF number for a fraud issue, you can create cases where the Fraud department is automatically set as the case owner.

## Access Cases in the agent application

After you enable Amazon Connect Cases, you need to take steps to make the functionality available through the agent application. This topic explains your options.

### Tip

Make sure your agents have **Cases** permissions in their security profile so they can access Cases. For more information, see [Security profile permissions for Cases](#).

### Option 1: Use Cases with the CCP out-of-the-box

Cases is already embedded alongside the Contact Control Panel (CCP). Your agents will access the CCP and Cases in the same browser window using a link that looks like this:

- `https://instance name.my.connect.aws/agent-app-v2/`

If you access your instance using the `awsapps.com` domain, use the following URL:

- `https://instance name.awsapps.com/connect/agent-app-v2/`

For help finding your instance name, see [Find your Amazon Connect instance name](#).

### Option 2: Embed Cases into a custom agent application

When you embed your Contact Control Panel (CCP), you have the option of showing or hiding the pre-built CCP user interface. For example, you may want to develop a custom agent application that has a user interface you design, with customized buttons to accept and reject calls. Or, you may want to embed the pre-built CCP that's included with Amazon Connect into another custom app.

You can display the pre-built CCP user interface, or hide it and build your own. In both scenarios, you can incorporate Cases into your agent application by using public APIs provided by Amazon
Connect. These APIs are built to provide you the flexibility to create the functionality and user experience that you want. For more information, see the Cases API documentation.

Tip

When you customize the agent's application, you determine what URL agents will use to access their agent application. This might be very different from the one provided by Amazon Connect. For example, your URL could be https://example-corp.com/agent-support-app.

Case event streams

Amazon Connect Cases event streams provide you with near real-time updates when cases are created or modified within your Amazon Connect Cases domain. The events published to the stream include these resource events:

- Case created
- Cases modified
- Related items (Comments, Calls, Chats, Tasks) are added to a case

You can use the case event streams to integrate streams into your data lake solutions, create dashboards that display case performance metrics, implement business rules or automated actions based on case events, and configure alerting tools to trigger custom notifications of specific case activity.

Contents

- Set up case event streams
- Case event payload and schema

Set up case event streams

This topic explains how to set up and use case event streams. Some of the onboarding steps require you to call Amazon Connect Cases APIs.
Step 1: Create an Amazon Connect instance and enable Customer Profiles

1. Ensure you have an working Amazon Connect instance in one of the AWS Regions where Cases is available. See Cases availability by Region.

2. Enable Amazon Connect Customer Profiles. For instructions, see Enable Customer Profiles for your instance.

Amazon Connect Cases requires Customer Profiles because each case must be associated with a customer profile from the Customer Profiles service.

Step 2: Add a Cases domain to your Amazon Connect instance

For instructions, see Enable Cases.

If you want to add a case domain using the API, see the CreateDomain API in the Amazon Connect Cases API Reference.

Step 3: Create a case template

Create a case template. In Step 6: Test case event streams, you'll use the template.

If you want to create a case template using the API, see the CreateTemplate API in the Amazon Connect Cases API Reference.

Step 4: Enable case event streams and setup to receive events into an SQS queue

Run the following command to enable case event streams for your Cases domain. After this command runs, when cases are created or updated, an event is published to the default-bus of the EventBridge service in your account (it must be in the same AWS Region as your Cases domain).

```
aws connectcases put-case-event-configuration --domain-id dad5efb6-8485-4a55-8241-98a88EXAMPLE --event-bridge enabled=true
```

By default, the events published by Amazon Connect Cases only contain metadata about the case, such as templateId, caseId, caseArn, approximateChangeTime, and more. You can run the following command to get more information about the case (at the time the event was generated) to be included in the event.

```
Set up case event streams
```
# You can include any other field defined in your cases domain in the fields section.
# To list the fields that are defined in your cases domain, call the Cases ListFields API.
# To include case fields that you create (custom fields) in the event, enter the custom field ID.

```bash
aws connectcases put-case-event-configuration --domain-id YOUR_CASES_DOMAIN_ID --event-bridge "{
  "enabled": true,
  "includedData": {
    "caseData": {
      "fields": [
        {
          "id": "status"
        },
        {
          "id": "title"
        },
        {
          "id": "customer_id"
        }
      ],
      "id": "your custom field ID"
    },
    "relatedItemData": {
      "includeContent": true
    }
  }
}
```

Next, create an Amazon SQS queue and set that as a target for the Amazon Connect Cases events on your EventBridge bus so that all the case events are delivered to the SQS queue for later processing.
# Create an SQS queue

```bash
"}"
```

# Create an rule on the EventBridge defualt bus that represents the case events

```bash
aws events put-rule --name case-events-to-sqs-queue --event-pattern "{"source": ["aws.cases"]}" --state ENABLED
```

# Ask event bridge to publish case events to the SQS queue.

```bash
aws events put-targets --rule case-events-to-sqs-queue --target "{"Id": "target-1", "Arn": "arn:aws:sqs:The AWS Region of your Amazon Connect instance:your AWS account ID:case-events-queue"}
```

**Step 5: Test case event streams**

Use the Amazon Connect agent application to:

1. Accept a chat contact.
2. Create a customer profile and associate that to the chat contact.
3. Create a case.

**Note**

The Create case button on the Cases tab is inactive until you accept a contact and associate that contact with a customer profile.

Navigate to the Amazon SQS console and check that a case event (type: CASE.CREATED) for the newly created case is available in your SQS Queue. Similarly, you can modify the case created above and get a corresponding case event (type: CASE.UPDATED) in your SQS queue. You can associate the contact to the case, and leave a comment on the case to get case events for those actions, too.
Step 6: Use cases for the case event streams

Case event streams publish events every time a case is created, case is updated, contact is associated to the case, and comment is added on a case. You can use these events for:

- Metrics, analytics and dashboards
- Build Apps that notify users (for example, send emails)
- Automated actions that are triggered based on certain type of case updates

For example, you can use the SQS target on EventBridge (as shown on step 4) to temporarily store the case events in the SQS queue, and use Lambda functions to process events in the SQS to build custom applications such as sending emails to the customer when their case is updated, automatically resolving any tasks linked to the case, and more. Similarly, you can use the Kinesis Data Firehose target on the EventBridge to store the case events into an S3 bucket and then use the AWS Glue for ETL, Athena for ad-hoc analytics, and Amazon QuickSight for dashboards.

Case event payload and schema

When you request to include case data in the event payload, the data reflects the version of the case after that particular edit.

Amazon Connect Cases default limits guarantee that the payload will be less than 256KB (the maximum size of an EventBus event). Since you can customize the case object model (for example, you can define custom fields on case objects to capture business specific information), case event schema reflect the customizations made to the case object as shown in the following examples (for example, see how customer-specific UUIDs are being use as JSON properties).

Example case event payload for the case resource

```json
// Given the limits on the "includedData" configuration
// this payload is guaranteed to less than 256KB at launch.
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Amazon Connect Cases Change",
    "source": "aws.cases",
    "account": "your AWS account ID",
    "time": "2022-03-16T23:43:26Z",
    "region": "The AWS Region of your Amazon Connect instance",
    "resources": [
```
"arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case domain ID",
"arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case domain ID/case/case ID"
]
,"detail": {
   "version": "0",
   "eventType": "CASE.UPDATED", // (or "CASE.CREATED" or "CASE.DELETED")
   "approximateChangeTime": "2022-03-16T23:16:57.893Z", // Can be used for ordering
   "changedFieldIds": ["status", "last_updated_datetime"],

   "case": {
      "caseId": "case ID",
      "templateId": "template ID",
      "createdDateTime": "2022-03-16T23:16:57.893Z",

      // This section contains only non-null field values for the fields that customers have configured in the "includedData".

      // Field values included in this section reflects the case after this particular change is applied.
      "fields": {
         "status": {
            "value": {
               "stringValue": "open"
            }
         },
         "case_reason": {
            "value": {
               "stringValue": "Shipment lost"
            }
         },
         "custom-field-uuid-1": {
            "value": {
               "stringValue": "Customer didn't receive the product"
            }
         }
      }
   }
}
Example case event payload for the related-item resource

```json
// Given the limits on the "includedData" configuration
// this payload is guaranteed to less than 256KB
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Amazon Connect Cases Change",
    "source": "aws.cases",
    "account": "your AWS account ID",
    "time": "2022-03-16T23:43:26Z",
    "region": "The AWS Region of your Amazon Connect instance",
    "resources": [
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case domain ID",
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case domain ID/case/case ID/related-item/related-item ID"
    ],

    "detail": {
        "version": "0",
        "eventType": "RELATED_ITEM.CREATED", //(or "RELATED_ITEM.UPDATED" or "CASE.RELATED_ITEM.DELETED")
        "approximateChangeTime": "2022-03-16T23:16:57.893Z", // Can be used for ordering
        "changedAttributes": ["comment.commentText"],

        "relatedItem": {
            "relatedItemType": "Comment", // (OR Contact)
            "relatedItemId": "related-item ID",
            "caseId": "case id that this related item is a sub-resource of",
            "createdDateTime": "2022-03-16T23:16:57.893Z",

            // This section includes any attributes that customers have configured
            // in the "includedData" configuration.
            "comment": {
                "body": "Gave a $5 refund to customer to make them happy",
            },

            // if the related item was of type contact.
            // "contact": {
            //     "contactArn": "........",
            // }
        }
    }
}
```
} 
} 
}
Amazon Connect Contact Lens

Note

Powered by Amazon Bedrock: AWS implements automated abuse detection. Because Amazon Connect Contact Lens is built on Amazon Bedrock, users can take full advantage of the controls implemented in Amazon Bedrock to enforce safety, security, and the responsible use of artificial intelligence (AI).

Amazon Connect Contact Lens provides contact center analytics and quality management capabilities that enable you to monitor, measure, and continuously improve contact quality and agent performance for a better overall customer experience.

- **Analyze conversations using conversational analytics.** You can uncover trends and improve customer service by understanding sentiment, conversation characteristics, emerging contact themes, and agent compliance risks.
- **Evaluate agent performance.** You can review conversations alongside contact details, recordings, transcripts, and summaries, without the need to switch applications. You can define and assess agent performance criteria (for example, script adherence, sensitive data collection, and customer greetings) and automatically pre-populate evaluation forms.
- **Set up and review agent screen recordings.** You can review agent actions handling customer contacts by reviewing screen recordings. This helps you ensure adherence to quality standards, compliance requirements, and best practices. It also helps you identify coaching opportunities and bottlenecks so you can streamline workflows.
- **Search for contacts.** You can search for contacts as far back as two years ago.
- **Monitor live and recorded conversations.** You can monitor live conversations (both voice and chat) and barge live voice conversations. This is especially helpful for agents in training.
- **Transfer, reschedule, or end** in-progress contacts. While on the **Contact details** page, you can manage in-progress contacts.

Contact Lens helps you protect your customer's privacy by enabling you to automatically redact sensitive data from conversation transcripts and audio files.
Analyze conversations using conversational analytics

With Amazon Connect Contact Lens, you can analyze conversations between customers and agents by using speech and chat transcriptions, natural language processing, and intelligent search capabilities. Amazon Connect Contact Lens performs sentiment analysis, detects issues, and enables you to automatically categorize contacts.

Speech analytics support

- **Real-time call analytics:** Use to detect and resolve customer issues more proactively while the call is progress. For example, it can **analyze and alert** you when a customer is getting frustrated because the agent is unable to resolve a complicated problem. This allows you to provide more immediate assistance.

- **Post-call analytics:** Use to understand trends of customer conversations and agent compliance. This helps you identify opportunities to coach an agent after the call.

Chat analytics support

- **Real-time chat analytics:** As with real-time call analytics, you can detect and resolve customer issues more proactively while the chat is progress and **receive an alert**. For example, managers can get a real-time email alert when customer sentiment for a chat contact turns negative, allowing them to join the in-progress contact and help resolve the customer issue.

- **Post-chat analytics:** Use to understand trends of customer conversations with both bots and agents. It provides information specific to a chat interaction, such as the agent greeting time, and agent and customer response times. The response times and sentiments help you investigate the customer's experience with the bot versus the agent, and identify areas for improvement.

You can protect your customer's privacy by redacting sensitive data, such as name, address, and credit card information from transcripts and audio recordings.

**Sample Contact details page for a call**

The following image shows the conversational analytics for a voice call. Notice that it includes **Talk time** metrics.
The following image shows the next section on the **Contact details** page for a voice call: the audio analysis and transcript. Notice that personally identifiable information (PII) has been **redacted from the transcript.**
Sample Contact details page for real-time chat analytics

The following image shows the conversational analytics for a real-time chat. Notice that it includes Key highlights and customer sentiment.

Sensitive information has been redacted from this conversation.
Sample Contact details page for post-chat analytics

The following image shows post-chat analytics. Notice that it includes chat response metrics, such as Agent greeting time (the time from the agent joining the chat to when they send the first response), Customer response time, and Agent response time.
The following image shows the next section on the **Contact details** page for a chat: the interaction analysis and transcript. Notice that you can investigate the customer’s interaction with a bot versus the agent.

---

**Note:**

Agent greeting time = after the agent joined the chat, how long until they sent the first response.
Enable Amazon Connect Contact Lens

You can enable Amazon Connect Contact Lens in a few steps. Add a `Set recording and analytics behavior` block to a flow, and configure it to enable Contact Lens for voice, chat, or both.

The following image shows a block that's configured for call recording, and Contact Lens speech analytics and chat analytics. The `Call recording` option is set to `Agent and customer`. In the `Analytics` section, the options are selected for speech and chat.

---

The customer’s interaction with system prompts or a bot is separated from their interaction with the agent, allowing you to investigate and improve it.
The procedures in this topic describe the steps to enable Contact Lens for call or chat analytics.

Contents

- **Important things to know**
- **Enable call recording and speech analytics**
- **Enable chat analytics**
- **Enable redaction of sensitive data**
- **Review sensitive data redaction for accuracy**
- **Dynamically enable Contact Lens using contact attributes**
- **Design a flow for key highlights**
- **What if the flow block fails to enable Contact Lens?**
- **Multi-party calls and Contact Lens**

**Important things to know**

- **Collect data after transferring a contact**: If you want to continue using Contact Lens to collect data after transferring a contact to another agent or queue, you need to add another **Set**
recording and analytics behavior block with Enable analytics enabled for the flow. This is because a transfer generates a second contact ID and contact record. Contact Lens needs to run on that contact record as well.

- When you select Enable Contact Lens conversational analytics, you must choose to enable speech or chat analytics. Otherwise, your flow will display an error when you publish it.

- Where you place the Set recording and analytics behavior block in a flow affects the agent's experience with key highlights. For more information, see Design a flow for key highlights.

Enable call recording and speech analytics

1. In the Set recording and analytics behavior block, under Call recording, choose On, Agent and Customer.

   Both agent and customer call recordings are required to use Contact Lens for voice contacts.

2. Under Analytics, choose Enable Contact Lens conversational analytics, Enable speech analytics.

   If you don't see this option, Amazon Connect Contact Lens hasn't been enabled for your instance. To enable it, see Update instance settings.

3. Choose one of the following:

   a. Post-call analytics: Contact Lens analyzes the call recording after the conversation and After Contact Work (ACW) is complete. This option provides the best transcription accuracy.

   b. Real-time analytics: Contact Lens provides both real-time insights during the call, and post-call analytics after the conversation has ended and After Contact Work (ACW) is complete.

   If you choose this option, we recommend setting up alerts based on keywords and phrases that the customer may utter during the call. Contact Lens analyzes the conversation real-time to detect the specified keywords or phrases, and alerts supervisors. From there, supervisors can listen in on the live call and provide guidance to the agent to help them resolve the issue faster.

   For information about setting up alerts, see Alert supervisors in real-time based on keywords and phrases mentioned during a call.
If your instance was created before October 2018, additional configuration is needed to access real-time call analytics. For more information, see Service-linked role permissions for Amazon Connect.

4. Choose the language. For a list of available languages for various Contact Lens features, see Supported languages.

For instructions on using an attribute, see Use contact attributes.

5. Optionally, enable redaction of sensitive data. For more information, see the next section, Enable redaction.

6. Choose Save.

7. If the contact is going to be transferred to another agent or queue, repeat these steps to add another Set recording and analytics behavior block with Enable Contact Lens for conversational analytics enabled.

Enable chat analytics

1. In the Set recording and analytics behavior block, under Analytics, choose Enable Contact Lens conversational analytics, and Enable chat analytics.

   ⚠️ Note
   By choosing this option you will receive both real-time and post-chat analytics.

If you don't see this option, Amazon Connect Contact Lens hasn't been enabled for your instance. To enable it, see Update instance settings.

2. Choose the language. For a list of available languages for various Contact Lens features, see Supported languages.

   For instructions on using an attribute, see Use contact attributes.

3. Optionally, enable redaction of sensitive data. For more information, see the next section, Enable redaction of sensitive data.

4. Choose Save.
5. If the contact is going to be transferred to another agent or queue, repeat these steps to add another Set recording and analytics behavior block with Enable Contact Lens for conversational analytics enabled.

Enable redaction of sensitive data

To enable redaction of sensitive data in a flow, choose Redact sensitive data. When redaction is enabled you can choose from the following options:

- Redact all personally identifiable information (PII) data (all PII entities supported).
- Choose which PII entities to redact from the list of supported entities.

If you accept the default settings, Contact Lens redacts all personally identifiable information (PII) it identifies, and replaces it with [PII] in the transcript. The default settings are shown in the following image because the following options are selected: Redact sensitive data, Redact All PII data, and Replace with placeholder PII.

Select PII entities to redact

Under the Data redaction section, you can select specific PII entities to redact. The following image shows that Credit/Debit Card Number is going to be redacted.
Choose data redaction replacement

Under the **Data redaction replacement** section, you can choose the mask to be used as data redaction replacement. For example, in the following image, the **Replace with placeholder PII** option indicates that PII will replace the data.

For more information about using redaction, see [Use sensitive data redaction](#).

Review sensitive data redaction for accuracy

The redaction feature is designed to identify and remove sensitive data. However, due to the predictive nature of machine learning, it may not identify and remove all instances of sensitive data in a transcript generated by Contact Lens. We recommend you review any redacted output to ensure it meets your needs.
**Important**

The redaction feature does not meet the requirements for de-identification under medical privacy laws like the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), so we recommend you continue to treat it as protected health information after redaction.

For the location of redacted files and examples, see [Output file locations](#).

**Dynamically enable Contact Lens using contact attributes**

You can dynamically enable Contact Lens and the redaction of the output files based on the language of the customer. For example, for customers using en-US, you may want only a redacted file whereas for those using en-GB, you may want both the original and redacted output files.

- **Redaction**: choose one of the following (they are case sensitive)
  - None
  - RedactedOnly
  - RedactedAndOriginal

- **Language**: Choose from the [list of available languages](#).

You can set these attributes in the following ways:

- **User defined**: use a **Set contact attributes** block. For general instructions about using this block, see [How to reference contact attributes](#). Define the **Destination key** and **Value** for redaction and language as needed.

  The following image shows an example of how you can configure the **Set contact attributes** block to use contact attributes for redaction. Choose the **Use text** option, set **Destination key** to `redaction_option`, and set **Value** to `RedactedAndOriginal`.

**Note**

**Value** is case sensitive.
Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

Contact attributes are accessible by other areas of Amazon Connect, such as the Contact Control Panel (CCP) and Contact Trace Records (CTRs).

Attribute to save

- Use text
  - Destination key
    - redaction_option
  - Value
    - RedactedAndOriginal
- Use attribute

The following image show how to use contact attributes for language. Choose the Use text option, set Destination key to language, set Value to en-US.
• **Use a Lambda function.** This is similar to how you set up user-defined contact attributes. An AWS Lambda function can return the result as a key-value pair, depending on the language of the Lambda response. The following example shows a Lambda response in JSON:

```json
{
    'redaction_option': 'RedactedOnly',
    'language': 'en-US'
}
```

### Design a flow for key highlights

Transcripts are visible to agents using the Contact Control Panel (CCP) depending on whether Contact Lens analytics is enabled in the **Set recording and analytics behavior** in the inbound flow, and/or a transfer flow.

This section provides three use cases for enabling Contact Lens analytics in the **Set recording and analytics behavior** block, and describes how they affect the agent's experience with key highlights.

### Use case 1: Contact Lens analytics is enabled in an inbound flow only

• A contact enters the inbound flow, and there are no call transfers. Following is the agent experience:

The agent receives the full transcript during After Contact Work (ACW). The transcript includes everything said by the agent and the customer, from the moment the agent accepts the initial call, until the call has ended, as shown in the following image.
• A contact enters the inbound flow, and there is a call transfer. Following is the agent experience:
  • Agent 1 receives a call transcript after they leave the conference/warm transfer, during ACW.

The transcript includes everything said by agent 1 and the customer, from the moment the agent accepts the initial call, until the agent 1 leaves the conference/warm transfer portion of the call. The transcript includes the flow (transfer/queue flow) prompt messages, as shown in the following image.

• Agent 2 receives a call transcript at the time of accepting the conference/warm transfer call from agent 1.

The transcript includes everything said by agent 1 and the customer, from the moment agent 1 accepts the initial call until the agent 1 leaves the conference/warm transfer portion of the
call. The transcript includes the flow (transfer/queue flow) prompt messages, and the warm transfer conversation, as shown in the following image.

Because Contact Lens is not enabled in the transfer flow, agent 2 doesn't see the remainder of the transcript when the call has ended and they enter ACW. The following image of ACW for agent 2 shows the transcript is empty.

Use case 2: Contact Lens analytics is enabled in an inbound flow and a transfer flow (quick connect)

- A contact enters the inbound flow, and there are no call transfers. Following is the agent experience:
• Agent 1 receives a full call transcript (unredacted) during ACW.

The transcript includes everything said by agent 1 and the customer from the moment the agent accepts the call, until the call has ended. This is shown in the following image of the CCP for agent 1.

![Call Transcript Example](image)

• A contact enters the inbound flow, and there is a call transfer. Following is the agent experience:
  • Agent 1 receives a call transcript after they leave the conference/warm transfer, during ACW.

  The transcript includes everything said by agent 1 and the customer from the moment agent 1 accepts the call, until agent 1 leaves the conference/warm transfer portion of the call. The transcript includes flow (transfer/queue flow) prompt messages.

  The full call transcript until warm transfer is shown in the following image.
Agent 2 receives a call transcript at the time of accepting the conference/warm transfer call from agent 1.

The transcript includes everything said by agent 1 and the customer, from the moment agent 1 accepts the call, until agent 1 leaves the conference/warm transfer portion of the call. The transcript includes the flow (transfer/queue flow) prompt messages.

Because Contact Lens is enabled in the transfer flow, agent 2 receives a call transcript after the call is completed, during ACW.

The transcript includes only the remaining portion of the call between agent 2 and customer, after agent 1 has left the call. The transcript includes everything said by agent 2 and the customer, from the moment they are conferenced/warm transferred in, until the call has ended. An example transcript is shown in the following image.
What if the flow block fails to enable Contact Lens?

It's possible that the [Set recording and analytics behavior](#) block can fail to enable Contact Lens on a contact. If Contact Lens isn't enabled for a contact, check the flow logs for the error.

Multi-party calls and Contact Lens

We do not support multi-party call architecture in Contact Lens. For example, if there are more than two parties (agent and customer) on a call, or a call is getting transferred to a third party, the quality of the transcription and analytics, such as sentiment, redaction, categories among others, can get degraded. We recommend you disable Contact Lens for multi-party or third-party calls if there are more than two parties (agent and customer). For information on disabling Contact Lens for a contact, see [Flow block: Set recording and analytics behavior](#).

Security profile permissions for Contact Lens

To keep customer data secure, you can set up permissions to have granular control on who can access information generated by Contact Lens.

The following image shows the [Analytics and Optimization](#) security profile permissions that apply to Contact Lens.
Following is a description of the permissions.

**Contact search**

This permission isn't specific to Contact Lens, but it is required so you can access the Contact search page, which is where you can search contacts so you can review the analyzed recording and transcript. In addition, you can do fast, full-text search on call transcripts, and search by sentiment score and non-talk time.

**View my contacts**

This permission isn't specific to Contact Lens, but it is required if you need to access the Contact search page, review only those contacts that you handled, and review the analyzed recording and transcripts.

**Important**

If both Contact search and View my contacts permissions are granted, then the user will have access to all contacts.

**Search contacts by conversation characteristics**

On the Contact Search page:
For voice contacts, you can access additional filters that allow you to return results by sentiment score and non-talk time.

For chat contacts, you can access an additional filter to search for contacts by response time.

For both voice and chat, you can search conversations that fall into specific contact categories.

For more information, see Search for sentiment score/shift, Search for non-talk time, and Search a contact category.

The following image shows the Filters section of the Contact Search page, and the Filters dropdown menu. Filters with CL next to them are only available to users who have this security profile permission.

Search contacts by keywords

On the Contact Search page, you can access additional filters that allow you to search contacts by Words or phrases, such as "thank you for your business." For more information, see Search for words or phrases.
Contact Lens - conversational analytics

On the Contact details page for a contact, you can view graphs that summarize conversational analytics: customer sentiment trend, sentiment, and talk time for voice contacts. For example, the following image shows how this information is displayed on the Contact details page for a voice contact.

Rules

This permission allows you to view, edit, or create rules for categorizing contacts. For more information, see Automatically categorize contacts based on keywords and phrases used during a conversation.

Recorded conversations (redacted)

On the Contact details and Contact search pages for a contact, this permission allows you to listen to call recording files or view the chat transcript in which the sensitive data has been removed. For more information, see Example redacted file for a call.
Recorded conversations (unredacted)

On the Contact details and Contact search pages, this permission manages access to unredacted content that contains sensitive data such as name and credit card information. It manages access to the following unredacted content:

- Original, unredacted chat and speech transcripts analyzed by Contact Lens
- Original, unredacted transcripts analyzed by Contact Lens
- Original, unredacted audio recordings

You can access this content on the Contact details page for a contact. For more information, see Example original, analyzed file for a call.

⚠️ Important

If you have permissions to both Recorded conversations (redacted) and Recorded conversations (unredacted), note the following behavior:

- By default only redacted recordings and transcripts are made available on the Contact details and Contact search pages.
- When no redacted content exists for the contact, or when redacted content cannot be shown to the user, then unredacted content is displayed on the Contact details and Contact search pages.

To access unredacted conversations, remove permissions to Recorded conversations (redacted). This leaves the user with only Recorded conversations (unredacted) permissions.

You cannot access both the redacted and unredacted version of a conversation at the same time.

Contact Lens notification types

Contact Lens provides the following notification types:

- Contact Lens Post Call/Chat Rules Matched: An EventBridge event is delivered whenever a Contact Lens rule is matched and has triggered the EventBridge rule action.

  This event contains useful information about the Contact Lens rule that is triggered including the category assigned, and details of the agent, contact and queue.
• Contact Lens Real Time Call/Chat Rules Matched: An EventBridge event is delivered whenever a Contact Lens rule is matched and has triggered in real time.

This event contains useful information about the Contact Lens rule that is triggered including the category assigned, and details of the agent, contact and queue.

• Contact Lens Analysis State Change: An EventBridge event is delivered when Contact Lens is unable to analyze a contact recording. The event contains the Event Reason Code which provides the details on why it was unable to process the recording.

You can use these notification types in a variety of scenarios. For example, use Contact Lens analysis State Change events to signal unexpected errors in the processing of a contact file where EventBridge event details can be subsequently stored in a CloudWatch log for additional review, trigger additional workflows, or alert relevant support teams for further investigation.

The Contact Lens events for speech and chat analytics enable numerous new use cases such as surfacing and visualization of additional insights, for example:

• Generate alerts on real-time customer sentiment drops across all call and chat conversations
• Aggregating and reporting on reoccurring issues and topics
• Measuring the impact of the latest marketing campaign by detecting how many customers referenced it during a call
• Customizing agent compliance standards for each Region and lines of business, and enrolling agents into additional training where required.

**Add custom vocabularies**

You can improve the accuracy of speech recognition for product names, brand names, and domain-specific terminology, by expanding and tailoring the vocabulary of the speech-to-text engine in Contact Lens.

This topic explains how to add custom vocabularies using the Amazon Connect admin website. You can also add them using the [CreateVocabulary](#) and [AssociateDefaultVocabulary](#) APIs.
Things to know about custom vocabularies

- You must set a vocabulary as the default for it to be applied to the analyses to generate transcripts. The following image shows the Custom vocabularies page. Choose the ellipsis, and then choose Set as default.

- You can have one vocabulary per language applied to the analyses. This means only one file per language can be in the Ready (default) state.

- You can upload more than 20 vocabulary files. However, you can activate only 20 custom vocabulary files at the same time.

- Transcription is a one-time event. A newly uploaded vocabulary isn't applied retroactively to existing transcriptions.

- Your text file must be in LF format. If you use any other format, such CRLF format, your custom vocabulary is not accepted by Amazon Transcribe.

- The sample vocabulary file can be downloaded only when you choose an English language setting.

- For limits to the size of a vocabulary file and other requirements, see Custom vocabularies in the Amazon Transcribe Developer Guide.

- Custom vocabularies apply to speech analytics only. They do not apply to chat conversations because the transcripts already exist.

Required permissions

Before you can add custom vocabularies to Amazon Connect, you need the Analytics and Optimization, Contact Lens - custom vocabularies permission assigned to your security profile.
By default, in new instances of Amazon Connect the **Admin** and **CallCenterManager** security profiles have this permission.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

**Add a custom vocabulary**

1. Log in to Amazon Connect with a user account that has the required permissions to add custom vocabularies.
2. Navigate to **Analytics and optimization, Custom vocabularies**.
3. Choose **Add custom vocabulary**.
4. On the **Add custom vocabulary** page, enter a name for the vocabulary, choose an English language, and then choose **Download a sample** file.

### Note

The sample vocabulary file can be downloaded only when you choose an English language setting. Otherwise, an error message is displayed, as shown in the following image.

The following image shows what the sample vocabulary file looks like. The header contains **Phrase**, **IPA**, **SoundsLike**, and **DisplayAs**. The header is required.
5. The information in the file is separated by one [TAB] per entry. For details about how to add words and acronyms to your vocabulary file, see Creating a custom vocabulary using a table in the Amazon Transcribe Developer Guide.

The following image shows words in a sample vocabulary file. Words in the Phrase column are required. Words in the IPA, SoundsLike, and DisplayAs columns are optional.

To enter multiple words in the Phrase column, separate each word with a hyphen (-); do not use spaces.

Vocabulary states

- **Ready (default)**: The vocabulary is being applied to the analyses to generate transcripts. It is applied to both real-time and post-call analyses.
- **Ready**: The vocabulary is not being applied to analyses, but it is a valid file and available. To apply it to analyses, set it to default.
- **Processing**: Amazon Connect is validating your uploaded vocabulary and trying to apply it to the analyses to generate transcripts.
- **Deleting**: You chose to Remove the vocabulary, and Amazon Connect is deleting it now.

It takes about 90 minutes for Amazon Connect to delete a vocabulary.

If you attempt to upload a vocabulary that does not validate, it results in a **Failed** state. For example, if you add multiple-word phrases to the Phrase column, and separate them with spaces instead of hyphens, it will fail.
Download and view a custom vocabulary

To view a custom vocabulary that has been uploaded, you download and open the file. Only files in the **Ready** state can be downloaded and viewed.

1. Navigate to **Analytics and optimization**, **Custom vocabularies**.
2. Choose **More**, **Download**. The location of **Download** is shown in the following image.

![Download Location](image)

3. Open the download to view the contents.
4. You can change the contents, and then choose **Save and upload**.

Create rules with Contact Lens

Contact Lens rules allow you to automatically categorize contacts, receive alerts, or generate tasks based on keywords that are used during a call or chat, sentiment scores, customer attributes, and other criteria.

This topic explains how to create rules using the Amazon Connect admin website. To create and manage rules programmatically, see **Rules actions** and the **Amazon Connect Rules Function language** in the **Amazon Connect API Reference Guide**.

**Tip**

For a list of rules feature specifications (for example, how many rules you can create), see **Amazon Connect Rules feature specifications**.

Step 1: Define rule conditions

1. On the navigation menu, choose **Analytics and optimization**, **Rules**.
2. Select **Create a rule, Conversational analytics.**

3. Under **When**, use the dropdown list to choose **post-call analysis, real-time analysis, or post-chat analysis.**

![Rules](image)

4. **Choose Add condition.**

You can combine criteria from a large set of conditions to build very specific Contact Lens rules. Following are the available conditions:

- **Words or phrases:** Choose from **Exact match, Pattern match, or Semantic match** to trigger an alert or task when keywords are uttered.

- **Agent:** Build rules that run on a subset of agents. For example, create a rule to ensure newly hired agents comply with company standards.

  To see agent names so you can add them to rules, you need **Users - View** permissions in your security profile.

- **Queues:** Build rules that run on a subset of queues. Often organizations use queues to indicate a line of business, topic, or domain. For example, you could build rules specifically for your sales queues, tracking the impact of a recent marketing campaign or alternatively rules for your customer support queues, tracking overall sentiment.

  To see the queue names so you can add them to rules, you need **Queues - View** permissions in your security profile.
• **Contact attributes**: Build rules that run on the values of custom contact attributes. For example, you can build rules specifically for a particular line of business or for specific customers, such as based on their membership level, their current country of residence, or if they have an outstanding order.

You can add up to five contact attributes to a rule.

• **Sentiment - Time period**: Build rules that run on the sentiment analysis results (positive, negative, or neutral) over a trailing window of time.

For example, you can build a rule for when customer sentiment has remained negative for a set period of time. If the participant joined the contact later, the time period set here applies to when participant was present.

• **Sentiment - Entire contact**: Build rules that run on the value of sentiment scores over an entire contact. For example, you can build a rule when customer sentiment has remained low for the entire contact, you can create a task for a customer experience analyst to review the call transcript and follow-up.

• **Interruptions**: Build rules that detect when the agent has interrupted the customer for more than X times. This feature applies to calls only.

• **Non-talk time**: Build rules that run when periods of no talk time are detected. For example, when a customer and agent have not spoken for over 30 seconds which may indicate unnecessary customer wait time or highlight a customer services process that would benefit from optimisation. This feature applies to calls only.

• **Response time**: Build rules to identify contacts where the participant had a response time longer or shorter than what was expected: Average or Maximum.

For example, you can set a rule on the Agent greeting time, also known as First response time: after the agent joined the chat, how long until they sent the first greeting message. This will help you to identify when an agent took too long to engage with the customer.

The following image shows a sample rule with multiple conditions for a voice contact.
The following image shows a sample rule with multiple conditions for a chat contact. The rule is triggered when the **First response time** is greater than or equal to 1 minute, and the agent did not mention any of the listed greeting words or phrases in their first response.

**First response time** = after the agent has joined the chat, how long until they sent the first message to the customer.
5. Choose **Next**.

**Step 2: Define rule actions**

1. Choose **Add action**. You can choose the following actions:

   - **Create Task**: this option is not available for real-time chat
   - **Send email notification**
   - **Generate an EventBridge event**
2. Choose **Next**.

3. Review and make any edits, then choose **Save**.

4. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

   You cannot apply rules to past, stored conversations.

**Automatically categorize contacts based on keywords and phrases used during a conversation**

You can set up Contact Lens to track issues that you know exist in your contact center ("known knowns"), and monitor any changes over time.

You can label your contacts based on predefined criteria you set up, that is, keywords and phrases you want to detect. Through categorization, each contact is analyzed for these criteria, and labeled.

This is useful to do when, for example, you want to ensure that agents are using certain words or phrases in calls or chats, for compliance reasons. Or, for example, you want to investigate when customers use certain words and have a negative sentiment.

To set up this feature, add rules that contain the words or phrases that you want to highlight.

In a **Contact details** page for a chat, categories appear above the transcript, as shown in the following image.
The following image shows what a **Contact details** page looks like with a category for a call. The category is named **cancellation**. It contains the words or phrases you want to highlight in the analysis.

Add rules to categorize contacts

**Step 1: Define conditions**

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. On the navigation menu, choose **Analytics and optimization**, **Rules**.
3. Select **Create a rule**, **Conversational analytics**.
4. Assign a name to the rule.
5. Under **When**, use the dropdown list to choose **post-call analysis**, **real-time analysis**, **post-chat analysis** or **real-time chat analysis**.
6. Choose **Add condition**, and then choose the type of match:

- **Exact Match**: Finds only the exact words or phrases. Enter the words or phrases, separated by a comma.

- **Semantic Match**: Finds words that may be synonyms. For example, if you enter "upset" it can match "not happy," or "hardly acceptable" can match with "unacceptable," and "unsubscribe" can match with "cancel subscription."

  Similarly, it can semantically match phrases. For example, "thank you so much for helping me out," "thanks a lot and this is so helpful," and "I am so happy that you are able to help me."

  This removes the need to define an exhaustive list of keywords while creating categories, and provides you the ability to cast a wider net for searching similar phrases that are important to you.

  For best semantic matching results, provide keywords or phrases with similar meaning within a semantic matching card. Currently, you can provide a maximum of four keywords and phrases per semantic matching card.

- **Pattern Match**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, if you are looking for contacts where the word "credit" was mentioned but you do not want to see any mention of the words "credit card,"
you can define a pattern matching category to look for the word "credit" that is not within a one-word distance of "card."

7. **Using Exact Match** as an example, enter the words or phrases, separated by a comma, that you want to highlight.

   ![Diagram showing how to use Exact Match to highlight words or phrases.]

8. **Choose Add.** Each word or phrase separated by a comma gets its own line in the card.

   ![Diagram showing the effect of adding words or phrases with commas.]

   The logic that Contact Lens uses to read these phrases is: (Hello OR thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business) OR (how OR may OR I OR assist OR you).

9. **To add more words or phrases, choose Add group of words or phrases.** In the following image, the first group of words or phrases are what the agent might utter, and the second group is what the customer might utter.
1. In this first card, Content Lens reads each line as an OR. For example: (Hello OR thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business) OR (how OR may OR I OR assist OR you).

2. The two cards are connected with an AND. This means, one of the rows in the first card needs to be uttered AND then one of the phrases in the second card needs to be uttered.

The logic that Contact Lens uses to read the two cards of words or phrases is (card 1) AND (card 2).

10. Choose **Add condition** to apply the rules to:

   - Specific queues
   - When contact attributes have certain values
   - When sentiment scores have certain values

For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for auto insurance, and the agent is located in Seattle.
Step 2: Define actions

In addition to categorizing a contact, you can define what actions Amazon Connect should take:

1. Generate an EventBridge event
2. Create Task
3. Send email notifications

Step 3: Review and save

1. When done, choose Save.
2. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

You cannot apply rules to past, stored conversations.

Alert supervisors in real-time based on keywords and phrases mentioned during a call

After you enable real-time analytics in your flow, you can add rules that automatically alert supervisors when a customer experience issue occurs.
For example, Contact Lens can automatically send an alert when certain keywords or phrases are mentioned during the conversation, or when it detects other criteria. The supervisor sees the alert on the real-time metrics dashboard. From there, supervisors can listen in to the live call, and provide guidance to the agent over chat to help them resolve the issue faster.

The following image shows an example of what a supervisor would see on the real-time metrics report when they get an alert. In this case, Contact Lens has detected an angry customer situation.

![Real-time metrics](image)

When the supervisor listens in to a live call, Contact Lens provides them with a real-time transcript and customer sentiment trend that helps them understand the situation and assess the appropriate action. The transcript also eliminates the need for customers to repeat themselves if they are transferred to another agent.

The following image shows a sample real-time transcript.
Add rules for real-time alerts for calls

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. On the navigation menu, choose **Analytics and optimization, Rules**.
3. Select **Create a rule, Conversational analytics**.
4. Assign a name to the rule.
5. Under **When**, use the dropdown list to choose **real-time analysis**.
6. Choose **Add condition**, and then choose the type of match:
   - **Exact Match**: Finds only the exact words or phrases.
   - **Pattern Match**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, you might look for contacts where the word "credit" was mentioned, but you do not want to see any mention of the words "credit card."
You can define a pattern matching category to look for the word "credit" that is not within a one-word distance of the word "card."

Tip
Semantic Match isn't available for real-time analysis.

7. Enter the words or phrases, separated by a comma, that you want to highlight. Real-time rules only support any keywords or phrases that were mentioned.

8. Choose Add. Each word or phrase separated by a comma gets its own line.

The logic that Contact Lens uses to read these words or phrases is: (Talk OR to OR your OR manager) OR (this OR is OR not OR helpful) OR (speak OR to OR your OR supervisor), etc.
9. To add more words or phrases, choose **Add group of words or phrases**. In the following image, the first group of words or phrases are what the agent might utter. The second group is what the customer might utter.

1. In this first card, Content Lens reads each line as an OR. For example: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business).

2. The two cards are connected with an AND. This means, one of the rows in the first card needs to be uttered AND then one of the phrases in the second card needs to be uttered.

The logic that Contact Lens uses to read the two cards of words or phrases is (card 1) AND (card 2).

10. Choose **Add condition** to apply the rules to:

- Specific queues
- When contact attributes have certain values
- When sentiment scores have certain values
For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for auto insurance, and the agent is located in Seattle.

11. When done, choose Next.

12. In the Assign contact category box, add a name for the category. For example, Compliant or Not_Compliant.

13. Choose Next, then choose Save and publish.

Alert supervisors in real-time based on keywords and phrases mentioned during a chat

After you enable real-time analytics in your flow, you can add rules that automatically alert supervisors when a customer experience issue occurs.

For example, Contact Lens can automatically send an alert when certain keywords or phrases are mentioned during the chat, or when it detects other criteria. The supervisor can then view the Contact details page for a real-time chat to view the issue. From there, supervisors can join the chat, and provide guidance to the agent over chat to help them resolve the issue faster.
The following image shows an example of what a supervisor would see on the **Contact details** page when they get an alert for a real-time chat. In this case, Contact Lens has detected an angry customer situation.

When the supervisor monitors a chat, Contact Lens provides them with a real-time transcript and customer sentiment trend that helps them understand the situation and assess the appropriate action. The transcript also eliminates the need for customers to repeat themselves if they are transferred to another agent.

**Add rules for real-time alerts for chats**

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. On the navigation menu, choose **Analytics and optimization, Rules**.
3. Select **Create a rule, Conversational analytics.**

4. Assign a name to the rule.

5. Under **When**, use the dropdown list to choose **real-time analysis.**

6. Choose **Add condition**, and then choose the type of match. The following image shows a rule configured for a **Sentiment - Time period** condition.

   Choose from the following options:
   
   - **Exact Match**: Finds only the exact words or phrases.
   
   - **Pattern Match**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, you might look for contacts where the word "credit" was mentioned, but you do not want to see any mention of the words "credit card."
You can define a pattern matching category to look for the word "credit" that is not within a one-word distance of the word "card."

**Tip**

Semantic Match isn't available for real-time analysis.

7. Enter the words or phrases, separated by a comma, that you want to highlight. Real-time rules only support any keywords or phrases that were mentioned.

8. Choose **Add**. Each word or phrase separated by a comma gets its own line.

The logic that Contact Lens uses to read these words or phrases is: (Talk OR to OR your OR manager) OR (this OR is OR not OR helpful) OR (speak OR to OR your OR supervisor), etc.
9. To add more words or phrases, choose **Add group of words or phrases**. In the following image, the first group of words or phrases are what the agent might mention. The second group is what the customer might mention.

![Image of Amazon Connect Content Lens interface]

1. In this first card, Content Lens reads each line as an OR. For example: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business).

2. The two cards are connected with an AND. This means, one of the rows in the first card needs to be mentioned AND then one of the phrases in the second card needs to be mentioned.

The logic that Contact Lens uses to read the two cards of words or phrases is (card 1) AND (card 2).

10. Choose **Add condition** to apply the rules to:
   - Specific queues
   - When contact attributes have certain values
   - When sentiment scores have certain values
For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for auto insurance, and the agent is located in Seattle.

11. When done, choose Next.

12. In the Assign contact category box, add a name for the category. For example, Compliant or Not_Compliant.

13. Choose Add action to specify what action Amazon Connect should take when the conditions are met. You can configure supervisor alerts by using email notifications or by developing a custom integration with EventBridge.
14. If you chose **Send email notification**, see Create Contact Lens rules that send email notifications for more details about completing the page and for information about email limits.

If you chose **Generate an EventBridge event**, see Create a Contact Lens rule that generates an EventBridge event for more details about completing the page and for information about subscribing to EventBridge event types.
Create Contact Lens rules that send email notifications

You can create Contact Lens rules that send email notifications to people in your organization. This helps you to respond more expeditiously to potential issues in your contact center. For example, you can create a rule to notify:

- A team supervisor when there is an account escalation or cancellation.
- A group of people in your contact center as a result of certain words being mentioned during a conversation.
- A designated person in your contact center when a disagreement occurs during the call.

All emails are sent from no-reply@amazonconnect.com.

**To create a Contact Lens rule that sends an email notification**

1. Log in to Amazon Connect with a user account that has the required permissions to create rules.
2. Navigate to Analytics and optimization, Rules.
3. On the Rules page, choose Create a rule, and then from the dropdown list, choose Conversational analytics.

4. On the New rule page, define the conditions for the rule. For more information, see **Step 1: Define conditions**.
5. When you define actions for the rule, choose Send email notification for the action.
6. In the **Send email notification** section, choose who is going to receive the email by using one of these options:
   
   - **Select recipients by login**: Routes the email to the specified user.
   - **Select recipients by tags**: Routes the email dynamically based on the agent's tag values.

   In the following image, the rule sends a notification email to the agent's team supervisor.

7. In **Subject**, add the email subject. In **Body**, add the contents of the email notification.

   To specify contact attributes in the body of the email, type `[` and a list of available attributes appears, as shown in the following image. The available attributes are **ContactId**, **AgentId**, **QueueId**, **RuleName**, and **instance_url**.
8. Choose Next. Review your selections, and then choose Save.

9. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

   You cannot apply rules to past, stored conversations.

**Email limits**

- Amazon Connect has a default limit of 500 emails a day. When that limit is exceeded, the Amazon Connect instance is blocked for 24 hours from sending more email. This is because the emails are subject to bounce and complaint limits. For more information, see the **Bounce** and **Complaint** sections in [Understanding email deliverability in Amazon SES](#).

- All emails are sent from no-reply@amazonconnect.com, which you cannot customize.

If the default option for sending emails does not meeting your requirements, please contact your Technical Account Manager or AWS Support to discuss with the Amazon Connect service team.

**Create a Contact Lens rule that generates an EventBridge event**

In real-time or post-call/chat, you can get events and use them to trigger subsequent notifications or alerts, or aggregate reports outside of Amazon Connect. There's a lot you can do with this data. For example:

- Get real-time alerts in a QuickSight dashboard.
- Create aggregated reported outside of Amazon Connect.
• Join data with your CRM.

• Connect your notification solution to EventBridge and make sure that by end of day, all of a certain type of events go to a certain inbox. The payload tells you the contact, agent, and queue.

To create a rule that generates an EventBridge event

1. When you create your rule, choose Generate EventBridge event for the action.

2. For **Action name**, enter the name for the event payload.

   **Note**

   The value you assign for **Action name** is visible in the EventBridge payload. When you aggregate events, the action name provides an additional dimension that you can use to process them. For example, you have 200 category names, but only 50 have a specific action name, such as NOTIFY_CUSTOMER_RETENTION.
3. Choose **Next**. Review and then **Save**.

4. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

   You cannot apply rules to past, stored conversations.

5. To leverage the EventBridge data, subscribe to the EventBridge event type. See the next procedure.

**Subscribe to EventBridge event types**

To subscribe to EventBridge event types, create a custom EventBridge rule that matches the following:

- "source" = "aws.connect"
- "detail-type" = "Contact Lens Analysis State Change" or one of the following:
  - **Contact Lens Post Call Rules Matched**
- Contact Lens Realtime Rules Matched
- Contact Lens Realtime Chat Rules Matched
- Contact Lens Post Chat Rules Matched
- Metrics Rules Matched

The following image shows these settings in the Event pattern section of the new rule page.

Example EventBridge payloads

Following is an example of what the EventBridge payload looks like when Contact Lens Post Call Rules Matched.

```json
{
    "version": "0", // set by EventBridge
    "id": "aaaaaaaa-bbbb-cccc-dddd-bf3703467718", // set by EventBridge
    "source": "aws.connect",
    "detail-type": "Contact Lens Post Call Rules Matched",
    "account": "your AWS account ID",
    "time": "2020-04-27T18:43:48Z",
    "region": "us-east-1", // set by EventBridge
}
```
"resources": ["arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN"],
"detail": {
    "version": "1.0",
    "ruleName": "ACCOUNT_CANCELLATION", // Rule name
    "actionName": "NOTIFY_CUSTOMER_RETENTION",
    "instanceArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN",
    "contactArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/contact/contact-ARN",
    "agentArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/agent/agent-ARN",
    "queueArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/queue/queue-ARN",
}

Following is an example of what the payload looks like when Contact Lens Realtime Rules Matched.

{
    "version": "0", // set by EventBridge
    "id": "aaaaaaaa-bbbb-cccc-dddd-bf3703467718", // set by EventBridge
    "source": "aws.connect",
    "detail-type": "Contact Lens Realtime Rules Matched",
    "account": "your AWS account ID",
    "time": "2020-04-27T18:43:48Z",
    "region": "us-east-1", // set by EventBridge
    "resources": ["arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN"],
    "detail": {
        "version": "1.0",
        "ruleName": "ACCOUNT_CANCELLATION", // Rule name
        "actionName": "NOTIFY_CUSTOMER_RETENTION",
        "instanceArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN",
        "contactArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/contact/contact-ARN",
        "agentArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/agent/agent-ARN",
        "queueArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/queue/queue-ARN",
    }
}
Create a task when a contact is categorized in real-time or post-call/chat

An especially powerful use of Content Lens rules is to build rules that generate tasks. This helps you identify issues in your contact center for you to follow up, and creates traceable actions with owners. Following are some examples:

- Create a task to review a contact when the customer is fraudulent. For example, you can create a follow-up task when a customer utters words or phrases that makes them appear potentially fraudulent.
- Follow up when the customer mentions specific topics that you want to later on upsell or provide additional support by reaching out.
- Follow up when there is a serious quality issue. In addition to contacts being categorized and getting alerts, you can route a task so you have owners. You also have contact records for these tasks, so you can search for and trace them.

To create a rule that creates a task

1. When you create your rule, choose Create Task for the action.

2. Complete the task fields as follows:
a. **Category name**: The category name appears in the contact record. Max length: 200 characters.

b. **Name**: The name appears in the agent's Contact Control Panel (CCP). Max length: 512 characters.

c. **Description**: The description appears in the agent's Contact Control Panel (CCP). Max length: 4096 characters.
In Name and Description, use [ ] to choose from a menu of dynamic values: ContactId, AgentId, QueueId, and RuleName. For more information, see Create a task when a contact is categorized in real-time or post-call/chat.

d. Task reference name: This is a default reference that automatically appears in the agent's CCP.
   
   - For real-time rules, the task reference links to the Real-time details page.
   - For post-call/chat rules, the task reference links to the Contact details page.

  e. Additional Reference name: Max length: 4096 characters. You can add up to 25 references.

  f. Select a flow: Choose the flow that is designed to route the task to the appropriate owner of the task. The flow must be saved and published for it to appear in your list of options in the dropdown.

3. The following image shows an example of how this information appears in the agent's CCP.
In this example, the agent sees the following values for **Name**, **Description**, and **Task reference name**:

a. **Name** = Action-Required-Contact Lens - ba2cf8fe....

b. **Description** = Test

c. **Task reference name** = taskRef and the URL to the Real-time details page

4. Choose **Next**. Review and then choose **Save** the task.

5. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

You cannot apply rules to past, stored conversations.

**Voice and task contact records are linked**

When a rule creates a task, a contact record is automatically generated for the task. It's linked to the contact record of the voice call or chat that met the criteria for the rule to create the task.

For example, a call comes into your contact center and generates CTR1:

```
Contact ID: CTR1-1234abc
Channel: Voice
Initiation method: Inbound

Category: Compliance
Custom Contact Attributes:
  • CustomerType: VIP
  • AgentLocation: NYC

Next contact ID: CTR2-5678abc
```
The Rules engine generates a task. In the contact record for the task, the voice contact record appears as the **Previous contact ID**. In addition, the task contact record inherits contact attributes from the voice contact record, as illustrated in the following image:

### Contact ID: CTR2-5678abc
- **Channel:** Task
- **Initiation method:** API
- **Category:** Compliance
- **Custom Contact Attributes:**
  - **CustomerType:** VIP  
  - **AgentLocation:** NYC
- **Previous contact ID:** CTR1-1234abc

---

**About dynamic values for ContactId, AgentId, QueueId, RuleName**

The dynamic values in brackets [ ] are called **contact attributes**. Contact attributes enable you to store temporary information about the contact so you can use it in a flow.

When you add contact attributes in brackets [ ] — such as ContactId, AgentId, QueueId, or RuleName — the value is passed from one contact record to another. You can use contact attributes in your flow to branch and route the contact accordingly.

For more information, see [Use Amazon Connect contact attributes](#).

### How to use a Word or phrase condition in a Contact Lens rule

When you add a condition to a Contact Lens rule, you have the option to specify a Words or phrases condition. You can choose Exact Match, Semantic Match, or Pattern Match for the words or phrases. This topic explains each type of match.

#### How to use exact match

**Exact Match** really is an exact word match, singular or plural.

#### How to use pattern match

If you want to match related words, append an asterisk (*) to the criteria. For example, if you want to match on all variations of "neighbor" (neighbors, neighborhood) you would type **neighbo***.

With **Pattern Match** you can specify the following:
• **List of values**: This is useful when you want to build expressions with interchangeable values. For example, the expression might be:

   *I’m calling about a power outage in ["Beijing" or "London" or "New York" or "Paris" or "Tokyo"]*

   Then in your list of values you would add the cities: Beijing, London, New York, Paris, Tokyo.

   The advantage of using values is that you can create one expression, instead of multiple. This reduces the number of cards that you need to create.

• **Number**: This option is used most frequently in compliance scripts, or if you’re looking for a context when you know somewhere in between there’s a number. This way you can put all of your criteria into one expression instead of two. For example, an agent compliance script might say:

   *I have been in this industry for [num] years and would like to discuss this topic with you.*

   Or a customer might say:

   *I have been a member for [num] years.*

• **Proximity definition**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, if you are looking for contacts where the word "credit" was mentioned but you do not want to see any mention of the words "credit card," you can define a pattern matching category to look for the word "credit" that is not within a one-word distance of "card."

   For example, a proximity definition might be:

   *credit* [is not within 0 to 1 word apart] *card*  

   Tip
   
   For a list of languages supported by pattern match, see [Pattern match languages](#).

**How to use semantic match**

Semantic matching is supported only for post-call/chat analysis.

• An "intent" is an example of utterance. It can be a phrase or a sentence.
• You can enter up to four intents in one card (group).

• We recommend using semantically similar intents within one card to get the best results. For example, there's a category for "politeness." It includes two intents: "greetings" and "goodbye". We recommend separating these intents into two cards:
  
  • Card 1: "How are you today" and "How's everything going". They are semantically similar greetings.
  
  • Card 2: "Thanks for contacting us" and "Thank you for being our customer." They are semantically similar goodbyes.

Separating the intents into two cards provides more accuracy than putting them all into one card.

**Enter a script in a rule**

There are times when you may need your agents to follow an exact script. For example, a compliance script that all agents need to follow.

To enter a script in a rule, enter phrases. For example, if you want to highlight when agents say *Thank you for being a member. We appreciate your business*, enter two phrases:

• Thank you for being a member.

• We appreciate your business.

To apply the rule to certain lines of businesses, add a condition for which queues it applies to, or contact attributes. For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for auto insurance, and the agent is located in Seattle.
Security profile permissions for Contact Lens rules

To view, edit, or add rules for automatic categorization, you must be assigned to a security profile that has **Analytics and Optimization: Rules** permissions.

To see agent names so you can add them to rules, you need **Users and permissions: Users - View** permissions in your security profile.

To see the queue names so you can add them to rules, you need **Routing: Queues - View** permissions in your security profile.

For more information, see [Security profile permissions for Contact Lens](#).

About contact attributes in a rule

You can have up to 5 contact attributes in a rule.

You can design flows to use the contact attributes you specify in a rule, and then route the task accordingly. For example, a call or chat arrives in your contact center. When Contact Lens analyzes the call or chat, it gets a hit on the **Compliance** rule. The contact record that's created for the call, for example, includes information similar to the following image. It shows the **Category** = **Compliance**, and it has two custom contact attributes: **CustomerType** = **VIP**, **AgentLocation** = **NYC**.
The Rules engine generates a task. The contact record for the task inherits the contact attributes from the voice contact record, as illustrated in the following image.

The voice contact record appears as the Previous contact ID.

The flow that you specify in the rule should be designed to use the contact attributes and route the task to the appropriate owner. For example, you may want to route tasks where CustomerType = VIP to a specific agent.

For more information, see Use Amazon Connect contact attributes.

Rules are applied to new contacts

After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

You cannot apply rules to past, stored conversations.

Error notifications: When Contact Lens can't analyze a contact

It's possible that Contact Lens can't analyze a contact file, even though analysis is enabled on the flow. When this happens, Contact Lens sends error notifications using Amazon EventBridge events.
Events are emitted on a **best effort** basis.

### Subscribe to EventBridge notifications

To subscribe to these notifications, create a custom EventBridge rule that matches the following:

- "source" = "aws.connect"
- "detail-type" = "Contact Lens Analysis State Change"

You can also add to the pattern to be notified when a specific event code occurs. For more information, see [Event Patterns](#) in the *Amazon EventBridge User Guide*.

The format of a notification looks like the following sample:

```json
{
   "version": "0", // set by CloudWatch Events
   "id": "55555555-1111-1111-1111-111111111111", // set by CloudWatch Events
   "source": "aws.connect",
   "detail-type": "Contact Lens Analysis State Change",
   "account": "111122223333",
   "time": "2020-04-27T18:43:48Z",
   "region": "us-east-1", // set by CloudWatch Events
   "resources": [
      "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-h9j0-7c822889931e",
      "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-h9j0-7c822889931e/contact/efgh4567-pqrs-5678-t9c0-111111111111"
   ],
   "detail": {
      "instance": "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-h9j0-7c822889931e",
      "contact": "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-h9j0-7c822889931e/contact/efgh4567-pqrs-5678-t9c0-111111111111",
      "channel": "VOICE",
      "state": "FAILED",
      "reasonCode": "RECORDING_FILE_CANNOT_BE_READ"
   }
}
```
## Event codes

The following table lists the event codes that may result when Contact Lens can't analyze a contact.

<table>
<thead>
<tr>
<th>Event reason code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVALID_ANALYSIS_CONFIGURATION</td>
<td>Contact Lens received invalid values when the flow was initiated, such as an unsupported or invalid language code, or an unsupported value for redaction behavior.</td>
</tr>
<tr>
<td>RECORDING_FILE_CANNOT_BE_READ</td>
<td>Contact Lens can't get the recording file. This might be because file isn't present in the S3 bucket, or there are problems with permissions.</td>
</tr>
<tr>
<td>RECORDING_FILE_TOO_SMALL</td>
<td>The recording file is too small for analysis (less than 105 ms). If file doesn’t have expected format, an INVALID error occurs. Empty JSON is also an unexpected object.</td>
</tr>
</tbody>
</table>
| RECORDING_FILE_TOO_LARGE                               | The recording file exceeds the duration limit for analysis.  
- Voice: More than 14,400 seconds, or 4 hours  
- Chat: More than 20K messages in a transcript         |
<p>| RECORDING_FILE_INVALID                                 | The recording file is invalid.                                                                                                             |
| RECORDING_FILE_Cannot_Be_Read                          | An error occurred when Contact Lens tried to read the recording file.                                                                      |
| RECORDING_FILE_EMPTY                                   | The recording file is empty.                                                                                                               |
| RECORDING_SAMPLE_RATE_NOT_SUPPORTED                    | The sample rate of the audio file is not supported. Contact Lens currently supports                                                          |</p>
<table>
<thead>
<tr>
<th>Event reason code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audio files with an 8kHz sample rate. That is the sample rate for Amazon Connect recordings.</td>
<td></td>
</tr>
</tbody>
</table>

**Error notifications: When Amazon Connect Rules action fails to run**

It's important to know when a specific rule action has failed in a production environment, and what caused the failure. Then you can proactively mitigate such failures in future.

To get real-time insights on the actions that failed to run, you integrate Amazon Connect Rules with Amazon EventBridge events. This enables you to be notified when, for example, the "Create task" action failed to run because the maximum number of **Concurrent active tasks per instance** reached the service quota. When this happens, Amazon Connect sends error notifications using Amazon EventBridge events.

Events are emitted on a **best effort** basis.

**Subscribe to EventBridge notifications**

To subscribe to these notifications, create a custom EventBridge rule that matches the following:

- "source" = "aws.connect"
- "detail-type" = "Contact Lens Rules Action Execution Failed"

You can also add to the pattern to be notified when a specific event code occurs. For more information, see [Event Patterns](#) in the *Amazon EventBridge User Guide*.

The format of a notification looks like the following sample:

```json
{
    "version": "0",
    "id": "8d122163-6c07-f8cb-06e7-373a1bcf8fc6",
    "source": "aws.connect",
    "detail-type": "Amazon Connect Rules Action Execution Failed",
    "account": "123456789012",
    "time": "2022-01-05T01:30:42Z",
    "region": "us-east-1",
```

Create rules with Contact Lens
Supported action types

- CREATE_TASK
- GENERATE_EVENTBRIDGE_EVENT
- SEND_NOTIFICATION

For information about ASSIGN_CONTACTCATEGORY, see Error notifications: When Contact Lens can't analyze a contact.

Supported trigger events

- REAL_TIME_CALL
- REAL_TIME_CHAT
- POST_CALL
- POST_CHAT
- THIRD_PARTY
Reason codes for failed actions

When an action fails, the error notification service collects the reason codes from the supported actions. For more information about the reason codes for Task and EventBridge action failures, see the following topics:

- For reason codes for Task action failures, see Errors in the StartTaskContact API topic in the Amazon Connect API Reference Guide.
- For reason codes for EventBridge action failures, see Errors in the PutEvents API topic in the Amazon EventBridge API Reference Guide.

JSONPath Reference for Rules action public API fields that support variable injection

When you create or manage rules programmatically using Amazon Connect APIs (such as CreateRule or UpdateRule), you can specify variables for certain parameters. The variables are resolved at runtime when the action is triggered, based on the value of the EventSourceName parameter.

For example, let's say you're setting up a task action and you want to add more context. Following is an example of how you could use variable injections to include the ID of the contact and the ID of the agent in the Description field of the task:

- Customer is unhappy about the phone call. A swear word was detected during the conversation with agent $.ContactLens.PostCall.Agent.AgentId in the contact $.ContactLens.PostCall.ContactId

When the action is triggered, his string would resolve to "Customer is unhappy about the phone call. A swear word was detected during a conversation with agent 12345678-1234-1234-1234-EXAMPLEID012 in the contact 87654321-1234-1234-1234-EXAMPLEID345"

The following table lists each event source, and the JSONPath to use for fields that support variable injection.

<table>
<thead>
<tr>
<th>EventSourceName</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnPostCallAnalysisAvailable</td>
<td>$.ContactLens.PostCall.ContactId</td>
</tr>
<tr>
<td>EventSourceName</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>OnRealTimeCallAnalysisAvailable</td>
<td>$.ContactLens.RealTimeCall.ContactId</td>
</tr>
<tr>
<td></td>
<td>$.ContactLens.RealTimeCall.Agent.AgentId</td>
</tr>
<tr>
<td></td>
<td>$.ContactLens.RealTimeCall.Queue.QueueId</td>
</tr>
<tr>
<td></td>
<td>$.ContactLens.PostChat.Agent.AgentId</td>
</tr>
<tr>
<td></td>
<td>$.ContactLens.PostChat.Queue.QueueId</td>
</tr>
<tr>
<td>OnSalesforceCaseCreate</td>
<td>$.ThirdParty.Salesforce.CaseCreate.CaseNumber</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Name</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Email</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Phone</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Type</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Subject</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.CreatedDate</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Salesforce.CaseCreate.Description</td>
</tr>
</tbody>
</table>
## Create alerts on real-time metrics

You can create rules that automatically send emails or tasks to managers based on the values of real-time metrics. This enables you to alert managers on contact center operations that could potentially impact the end-customer experience. For example, you can set up an alert that sends an email to a manager when one or more agents on their team have been on break for longer than 30 minutes.

### Contents

- [Step 1: Define rule conditions](#)
- [Step 2: Define rule actions](#)

### Step 1: Define rule conditions

1. On the navigation menu, choose **Analytics and optimization**, **Rules**.
2. Select **Create a rule, Real-time metrics**.
3. Under **When**, use the dropdown list to choose from three event sources: **There is an update in queue metrics**, **There is in update in routing profile metrics**, **There is an update in agent metrics**. These options are shown in the following image.

<table>
<thead>
<tr>
<th>EventSourceName</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnZendeskTicketCreate</td>
<td>$.ThirdParty.Zendesk.TicketCreate.Id</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Zendesk.TicketCreate.CreatedAt</td>
</tr>
<tr>
<td>OnZendeskTicketStatusUpdate</td>
<td>$.ThirdParty.Zendesk.TicketStatusUpdate.Id</td>
</tr>
<tr>
<td></td>
<td>$.ThirdParty.Zendesk.TicketStatusUpdate.CreatedAt</td>
</tr>
</tbody>
</table>
4. Choose **Add condition**. The **Metrics** card is added automatically, as shown in the following image.

**Note**

- You can add up to 2 Metrics cards. This enables you to create a condition where one card evaluates real-time metrics and another evaluates trailing windows of time. For example, you may want an alert when several agents on are lunch break...
(Agent activity = Lunch break for 1 hour) and Average handle time is greater than 5 minutes.

- You can add up to 10 metrics to each **Metrics** card.

Following are the available real-time metrics you can add, depending on the event source.

- **There is an update in queue metrics - real-time**
  - **Contacts in queue**: Build rules that run when the number of contacts in a queue is a specified value.
  - **Oldest contact age**: Build rules that run when the oldest contact in queue reaches a specified age.
  - **Agents available**: Build rules that run when the number of agents available to handle contacts reaches a specified value.

The following image shows a condition that is met when **Contacts in queue** is greater than or equal to 400 AND **Oldest contact agent** is greater than or equal to 10 minutes AND **Agents available** is greater than or equal to 0, for the **Basic Routing Profile**.

To evaluate the condition with OR instead of AND, change the **Logic** setting to **Any**.

- **There is an update in queue metrics - trailing windows of time**

  Trailing windows of time is the past x minutes or hours.
- **Average handle time**: Build rules that run when the average handle time reaches a specified duration.
- **Average queue answer time**: Build rules that run when the average queue answer time reaches a specified duration.
- **Average agent interaction time**: Build rules that run when the average interaction time reaches a specified duration.
- **Average customer hold time**: Build rules that run when the average hold time reaches a specified duration. This metric does not apply to tasks so the value for them is always 0.
- **Service level**: Build rules that run when the service level reaches a specified percent.

There is an update in routing profile metrics

Trailing windows is not available for rules based on routing profiles.

- **Agents available**: Build rules that run when the number of agents available to take inbound contacts reaches a specified value.

There is an update in agent metrics - real-time

- **Agent activity**: Build rules that run when the agent activity equals a certain value such as Available, Incoming, On contact, and more.

There is an update in agent metrics - trailing windows

- **Average handle time**: Build rules that run when the Average handle time historical metric reaches a specified duration.
  
- **Agent occupancy**: Build rules that run when the Occupancy historical metric reaches a specified percent.

5. Choose **Next**.

**Step 2: Define rule actions**

1. Choose **Add action**. You can choose the following actions:

   - **Create Task**
   - **Send email notification**
   - **Generate an EventBridge event**: Use **Metrics Rules Matched** for the detail type.
2. Choose **Next**.

3. Review and make any edits, then choose **Save**.

4. After you add rules, they are applied to new evaluation submissions that occur after the rule was added. You cannot apply rules to past, stored evaluations.

**Search conversations analyzed by Contact Lens**

You can search the analyzed and transcribed recordings based on:

- Speaker (agent or customer)
- Keywords
- Sentiment score
- Non-talk time (for calls only)
- Response time (for chats only)

In addition, you can search conversations that are in specific contact categories (that is, the conversation has been categorized based on uttered keywords and phrases).

These criteria are described in the following sections.
Important

When a Contact Lens is enabled on a contact, after a call or chat ends and the agent completes After Contact Work (ACW), Contact Lens analyzes (and for calls, transcribes) the recording of the customer-agent conversation. The agent must choose Close contact first. Chat transcripts are indexed for search when Contact Lens is enabled; they are not indexed for search if Contact Lens is not enabled.

Required permissions for searching conversations

Before you can search conversations, you need the following permissions in your security profile. They allow you to do the type of search you want.

- Enable one of the following permissions to access the Contact Search page:
  - Contact search. Allows you to search for all contacts.
  - View my contacts: Allows you to search for only those contacts that you handled as an agent.
  - Search contacts by conversation characteristics. This includes non-talk time, sentiment score, and contact category.
  - Search contacts by keywords

For more information, see Security profile permissions for Contact Lens.

Search for words or phrases

For keyword search, Contact Lens uses the standard analyzer in Amazon OpenSearch Service. This analyzer is not case sensitive. For example, if you enter thank you for your business 2 CANCELLED Flights, the search looks for:

[thank, you, for, your, business, 2, cancelled, flights]

If you enter “thank you for your business”, two, ”CANCELLED Flights”, the search looks for:

[thank you for your business, two, cancelled flights]

To search conversations for words or phrases

1. In Amazon Connect, log in with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Search contacts by keywords permission.
2. Choose **Analytics and optimization, Contact search**.

3. In the **Filter** section, specify the time period that you want to search, and specify the channel.

   ![](image1.png)

   **Tip**
   When searching by date, you can search up to 8 weeks at a time.

4. Choose **Click here to add filter**, and in the dropdown menu, choose **Words or phrases**.

5. In the **Used by** section, choose whose part of the conversation you want to search. Note the following:

   - **System** applies to chat, where the participant may be a Lex bot or prompt.
   - To search for words or phrases that are used by all participants, select **Agent, Customer, System**.
   - If no boxes are selected, it means search for words or phrases used by any of the participants.

6. In the **Logic** section, choose from the following options:

   - Choose **Match any** to return contacts that have any of the words present in the transcripts.

     For example, the following query means match (hello OR cancellation OR "example airline"). And, because no **Used by** boxes are selected, it means "find contacts where any of these words were used by any of the participants."
Choose **Match all** to return contacts that have all of the words present in the transcripts.

For example, the following query means match ("thank you for your business" AND cancellation AND "example airline"). And, because all the participant boxes are selected, it means “find contacts where all of these words and phrases were used by all of the participants.”

7. **In the Words or phrases section,** enter the words to search, separated by commas. If you enter a phrase, surround it with quotation marks.

You can enter up to 128 characters.
Search for sentiment score or evaluate sentiment shift

With Contact Lens, you can search conversations for sentiment scores or sentiment shifts on a scale of -5 (most negative) to +5 (most positive). This enables you to identify patterns and factors for why calls go well or poorly.

For example, suppose you want to identify and investigate all the contacts where the customer sentiment ended negatively. You might search for all contacts where the sentiment score is $\leq -1$.

For more information, see Investigate sentiment scores during contacts.

To search for sentiment scores or evaluate sentiment shift

1. In Amazon Connect, log in with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Search contacts by conversation characteristics permission.

2. On the Contact search page, specify whether you want the sentiment score for words or phrases spoken by the customer or agent.

3. In Type of score analysis, specify what type of scores to return:

   - **Sentiment score**: This returns the average score for the customer or agent's portion of the conversation.

   In addition to searching for sentiment scores when the agent or customer are on the contact, you can filter the search by when the customer is:

   - **With agent on the chat**
   - **Without agent on the chat**: This is the time the customer is chatting with a bot, prompts, and time in queue.
• **Sentiment shift**: Identify where the customer or agent's sentiment changed during the contact.

For example, the following images shows an example of searching for contacts where the customer's sentiment score begins at less than or equal to -1 and ends at greater than or equal to +1. In addition, the customer is on a chat with the agent present.

---

**Search for non-talk time**

To help you identify which calls to investigate, you can search for non-talk time. For example, you might want to find all calls where the non-talk time is greater than 20%, and then investigate them.

Non-talk time includes hold time and any silence where both participants aren't talking for longer than three seconds. This duration can't be customized.
Use the drop-down arrow to specify whether to search conversations for the duration or percentage of non-talk time. These options are shown in the following image.

For information about how to use this metric, see Investigate non-talk time during calls.

Search by response time for chat conversations

You can search by the:

- Average response time of the agent or customer during the chat
- Maximum response time of the agent or customer during the chat

You specify whether the duration is less or greater than or equal to a specific time. For information about how to use this metric, see Investigate response time during chats.

For the supported minimum and maximum response times, see Amazon Connect Rules feature specifications.

The following image shows a search for contacts where the agent's average response time was greater than or equal to 1 minute.
Search a contact category

1. On the Contact search page, choose Add filter, Contact category.

2. In the Contact categories box, use the dropdown box to list all the current categories that are available for you to search. Or, if you start typing, the input is used to match existing categories and to filter those that don't match.

- **Match any**: Searches for contacts that match any of the selected categories.
- **Match all**: Searches for contacts that match all of the selected categories.
- **Match none**: Searches for contacts that did not match any of the selected categories. Note that this would only return contacts that were analyzed by Contact Lens conversational analytics.

The following image shows a dropdown menu with all the current categories listed.
Review analyzed conversations using Contact Lens

By using Amazon Connect Contact Lens, you can review the transcript and identify what part of the contact is of interest. You won't need to listen to an entire call or read an entire chat transcript to find out what's interesting about it. You can focus on specific parts of the audio or transcript. Both are highlighted for you wherever there are points of interest.

For example, you might scan the transcript of the contact and see a red sentiment emoji for a customer turn, which indicates the customer is expressing a negative sentiment. You can choose the timestamp and jump to that portion of audio recording or chat interaction.

The following image shows an example of a voice contact.
The following image shows an example of a chat contact. **System Message** applies to chat, where the participant may be a Lex bot or prompt.

### To review analyzed conversations

1. Log in to Amazon Connect with a user account that has **Contact search** and **Contact Lens - conversational analytics** permissions in the security profile.
2. In Amazon Connect, choose **Analytics and optimization, Contact search**.
3. Use the filters on the page to narrow your search for a contact. For date, you can search up to 14 days at a time. For more information about searching for contacts, see [Search for contacts](#).
4. Choose the contact ID to view the contact details for the contact.
5. In the **Recording** and **Transcript** sections of the **Contact details** page, review what was spoken or written, when, and their sentiment.
6. For calls, if desired, choose the play prompt to listen to the recording. Or, click on the relevant part of the recording to listen to the portion you're interested in.

7. For chats, if desired, use the graph to navigate to the portion of the transcript you're interested in.

Quickly navigate transcripts and audio

Supervisors are often required to review the contacts for many agents, for quality assurance purposes. The turn-by-turn transcript and sentiment data helps you quickly identify and navigate to the portion of the recording that is of interest to you.

The following image of a contact record shows features that enable you to quickly navigate transcripts and audio to find areas that need your attention. While the image shows a voice contact, the same features apply to chat contacts.

1. Use Show key highlights to review only the issue, outcome, and/or action item.
2. Use **Autoscroll** for voice contacts, to jump around the audio or transcript. The two always stay in sync.

3. Scan for **sentiment emojis** to quickly identify a part for the transcript you want to read or listen to.

4. Choose the timestamp to jump to that part of the audio recording or transcript. The timestamp is calculated from the start of the customer interaction within the contact.

**Show key highlights**

It can be time-consuming to review contact transcripts that are hundreds of lines long. To make this process faster and more efficient, Contact Lens provides the option for you to view key highlights. The highlights show only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript.

- **Issue** represents the call driver. For example, "I'm thinking of upgrading to your online subscription plan."

- **Outcome** represents the likely conclusion or outcome of the contact. For example, "Based on your current plan I would recommend the online essentials plans that we have."

- **Action item** represents the action item the agent takes. For example, "Please keep an eye out for an email with a price quote. I will send it to you shortly."

Each contact has no more than one issue, one outcome, and one action item. Not all contacts will have all three.

**Note**

If Contact Lens displays the message **There are no key highlights for this transcript**, it means no issue, outcome, or action item was identified.

You don't need to configure key highlights. It works out-of-the-box without any training of the machine learning model.

**Turn on autoscroll to synchronize the transcript and audio**

For voice contacts, use **Autoscroll** to jump around the audio or transcript, and the two always stay in sync. For example:
• When you listen to a conversation, the transcript moves along with it, showing you sentiment emojis and any detected issue.
• You can scroll through the transcript, and choose the timestamp for the turn to listen to that specific point in the recording.

Because the audio and transcript are aligned, the transcript can help you understand what the agent and customer are saying. This is especially useful when:

• The audio is bad, maybe due to a connection issue. The transcript can help you understand what's being said.
• There's a dialect or language variant. Our models are trained on different accents so the transcript can help you understand what's being said.

**Scan for sentiment emojis**

Sentiment emojis help you quickly scan a transcript so you can listen to that part of the conversation.

For example, where you see red emojis for customer turns and then a green emoji, you might choose the timestamp to jump to that specific point of the conversation to check how that agent helped the customer.

**Tap or click category tags to navigate through transcript**

When you tap or click on the category tags, Contact Lens auto-navigates to the corresponding point-of-interests in the transcript. There are also category markers in the visualization of the interaction to indicate which part of the recording file has utterances related to the category.

The following image shows part of a **Contact details** page for a chat.
You can save valuable time with generative AI–powered summaries that provide essential information from customer conversations in a structured, concise, and easy to read format. You can quickly review the summaries and understand the context instead of reading through transcripts and monitoring calls.

Region and language availability: This preview release is available in the US East (N. Virginia) and US West (Oregon) AWS Regions, and in English locales. It’s available for the voice and chat channels.

The following shows an example of post-contact summarization powered by generative AI on the Contact details page.
The following image shows an example of post-contact summarization powered by generative AI on the Contact search page.

Each contact has no more than one summary generated. Not all contacts will have a summary generated.

**Note**

Chat contacts in supported locales and AWS Regions have summaries only for text/plain messages.
Get started

Perform the following steps to access and enable the preview release of post-contact summarization powered by generative AI.

Step 1: Sign up for the preview

1. This feature is only available in preview. To access this preview, complete the Gated product preview page request form.
2. After we review your sign-up form, we'll contact you with next steps.
3. After your Amazon Connect instance is allow-listed to use this feature in preview, perform the following steps to enable the feature.

Step 2: Enable contact for post-contact summarization powered by generative AI

To apply this feature to a contact that is enabled for Contact Lens conversational analytics, you must set a user user-defined attribute named connect:post-contact-summary-public-preview to true before contact terminates. Perform the following steps.

1. Add a Set contact attributes block to your flow.
2. Configure the Properties page of the block:
   - Namespace = User defined
   - Key = connect:post-contact-summary-public-preview
   - Value = true

An example Properties page is shown in the following image:
Note

For information about the service quota for this preview release, see Concurrent post-contact summarization jobs in Amazon Connect service quotas.

Step 3: Assign security profile permissions

Assign the following security profile permissions to users who need access to this feature:
- Contact Lens–post-contact summary, View
- Recorded conversations (redacted), View or Recorded conversations (unredacted), View

The following image shows where these permissions are located on the **Analytics and Optimization** section of the **Edit security profile** page.

---

**View key highlights**

It can be time-consuming to review contact transcripts that are hundreds of lines long. To make this process faster and more efficient, Contact Lens automatically identifies and labels key parts of customer conversations, then displays highlights of the conversations. Managers can view those
highlights on the **Contact details** page. Agents can view the highlights in the Contact Control Panel (CCP).

**Tip**
For a list of supported languages, see the *Key highlights* column in the Amazon Connect Contact Lens supported languages topic.

After you enable Contact Lens, it identifies key parts of a customer conversation, assigns labels (such as issue, outcome, or action item) to those parts, and displays highlights of the customer conversation. You can expand the highlights to view the full transcript of the contact.

The following example shows the key highlights on the **Contact details** page.

1. **Toggle** *Show key highlights* on and off as needed.
2. **Issue** represents the contact driver. For example, "I'm thinking of upgrading to your online subscription plan."
3. **Action item** represents the action item the agent takes. For example, "Please keep an eye out for an email with a price quote. I will send it to you shortly."
4. **Outcome** represents the likely conclusion or outcome of the contact. For example, "Based on your current plan I would recommend our online essentials plan."
Contacts have only one issue, one outcome, and one action item. It's possible for some contacts to not have all three.

Note
You see this message **There are no key highlights for this transcript** when Contact Lens can't identify an issue, outcome, or action item.

To learn about the agent's experience—what part of the transcript is displayed in the Contact Control Panel (CCP), and when—see [Design a flow for key highlights](#).

**Use theme detection to discover issues**

Use theme detection to discover previously unknown or emerging contact themes from thousands of customer interactions. For example, you can spot common reasons for customer outreach such as "cancel reservation" or "delayed order." You can then take appropriate actions to improve the customer experience by expediting issue resolution, and improving IVR options, knowledge base articles, and agent training.

**Important things to know**

- Theme detection is available in some languages supported by Amazon Connect Contact Lens. For more information, see [Languages supported by Amazon Connect Contact Lens](#).
- Theme detection is supported on contacts that were created on or after January 30, 2023.
- The **Generate themes report** button is enabled only when your saved search contains at least 1,000 contacts with issues detected by Contact Lens.
- The theme detection report is generated for the 3,000 most recent contacts.
- Theme detection reports are available for 30 days after they are created. After 30 days, the reports are deleted from the database and cannot be retrieved.
- The most recent 20 theme reports for a saved search are available in the **View theme reports** dropdown menu, as shown in the following image.
How to generate a theme report

1. Login to Amazon Connect using an account that has the following security profile permissions:
   - **Contact search - Access**
   - **Contact Lens - theme detection - Create**
   - **Contact Lens - theme detection - View**

2. In Amazon Connect, on the left navigation menu, choose **Analytics and optimization, Contact search**.

3. On the **Contact search** page, apply filters to select a group of contacts that have been analyzed by Contact Lens.

   **Important**
   Your search query must return at least 1,000 contacts with issues detected by Contact Lens. Otherwise, the **Generate themes report** button is not enabled.

4. Choose **Save search** to save your results. Assign a name to your search.

5. Choose **Generate themes report**.

   Contact Lens applies machine learning to automatically group contacts with similar issues. When the report is generated, a banner displays a link to the theme report. An example banner is shown in the following image.
6. Click or tap the link for the theme report.

   The theme report is displayed. It includes theme labels and a list of contacts, as shown in the following image.

7. Click or tap the theme labels to view associated contacts, listen to specific recordings, and read transcripts for deeper analysis.
Investigate sentiment scores during contacts

What are sentiment scores?

A sentiment score is an analysis of text, and a rating of whether it includes mostly positive, negative, or neutral language. Supervisors can use sentiment scores to search conversations and identify contacts that are associated with varying degrees of customer experiences, positive or negative. It helps them identify which of their contacts to investigate.

You can view a sentiment score for the entire conversation, as well as sentiment trend across whole contact.

How to investigate sentiment scores

When working to improve your contact center, you may want to focus on the following:

• Contacts that start with a positive sentiment score but end with a negative score.

  If you want to focus on a limited set of contacts to sample for quality assurance, for example, you can look at contacts where you know the customer had a positive sentiment at the start but ended with a negative sentiment. That shows you they left the conversation unhappy about something.

• Contacts that start with a negative sentiment score but end positive.

  Analyzing these contacts will help you identify what experiences you can recreate in your contact center. You can share successful techniques with other agents.

An additional way of looking at sentiment progression is to check the sentiment trendline. You can see the variation in the customer's sentiment as the contact progresses. For example, the following image shows a conversation with a very low sentiment score in the beginning of the conversation, and very positive one at the end.
For more information, see Search for sentiment score or evaluate sentiment shift.

**How sentiment scores are determined**

Amazon Connect Contact Lens analyzes the sentiment of each speaker turn in a conversation as positive, negative, or neutral. It then considers two factors for each participant turn to assign a score that ranges from -5 to +5 for each period of the call:

- **Frequency.** The number of times the sentiment is positive, negative or neutral.
- **Sentiment streaks.** The consecutive turns with same sentiment.

The overall sentiment score is the average of the scores assigned during each portion of the call.

**Investigate non-talk time during calls**

**What is non-talk time?**

Amazon Connect Contact Lens also identifies the amount of *non-talk time* in a call. Non-talk time equals hold time, plus any silence where both participants aren't talking for more than 3 seconds. This duration can't be customized.

The following image shows the location of non-talk time data on the **Contact details** page.
How to investigate non-talk time

Non-talk time can help you identify calls that have gone poorly. This may be because:

- The customer was asking a question that's new for your contact center.
- It's taking the agent a long time to do something but they are well-trained. This indicates there may be an issue with the tools the agent is using. For example, the tools aren't responsive enough or aren't easy to use.
- The agent didn't have a ready answer, but they are fairly new. This indicates they need more training.

You can decide whether to focus on these contacts to improve your contact center. For example, you can go to that section of the audio, and then look at the transcript to see what was going on.

In the following example, the non-talk time occurred when the agent was searching for the caller's trip ID. This could indicate there's an issue with the agent's tools. Or if the agent is new, they need more training.
For more information, see [Search for non-talk time](#).

**Investigate response time during chats**

Use the response time metric to understand the responsiveness of the agent or customer during a chat contact.

Contact Lens calculates the following metrics:

- **Agent greeting time.** This is the first response time for the agent, which is how fast the agent engaged with the customer after the agent joined the chat. A long first response time may explain, for example, if a customer has a negative sentiment in the beginning of conversation.

- **Avg agent response time** and **Avg customer response time.** The agent response time helps you check an agent's performance against your organization's base line.

- **Max agent response time** and **Max customer response time.**

  The customer's max response time may explain an agent's response time. For example, if a customer didn't reply for five minutes and then sent a message, it's possible the agent took longer than usual to respond because they were handling other chats at the same time.

We recommend examining the response time metrics in conjunction with the interactions graph that shows gaps in conversation and participant sentiment.
You can click or tap the longest response time value on the graph to be directed to the associated message in the transcript.

The following image of the Contact details page shows metrics for chat conversations. Note that Agent greeting time = after the agent joined the chat, how long until they sent the first response.

For more information, see Search by response time for chat conversations.

Investigate loudness scores during calls

A loudness score measures how loudly the customer or agent are speaking during a call. Contact Lens displays an analysis of the conversation that lets you identify where the customer or agent may be talking loudly and have a negative sentiment.

How to use loudness scores

We recommend using loudness scores together with sentiments. Look for areas of the conversation where the loudness score is high and the sentiment is low. Then read that portion of the transcript or listen to that section of the call.
For example, the following is an image of a recording and transcript analysis. Spiked vertical bars indicate where the customer is talking loudly. The horizontal red bars indicate their sentiment is negative.

**Use sensitive data redaction**

To help you protect your customer's privacy, Contact Lens lets you automatically redact sensitive data from conversation transcripts and audio files. It redacts sensitive data, such as name, address, and credit card information using Natural Language Understanding.

To enable redaction, choose the option on the **Set recording and analytics behavior** block. For more information, see [Enable redaction of sensitive data](#).

Sensitive data redaction is applied after a call disconnects.

⚠️ **Important**

The redaction feature is designed to identify and remove sensitive data. However, due to the predictive nature of machine learning, it may not identify and remove all instances of sensitive data in a transcript generated by Contact Lens. We recommend you review any redacted output to ensure it meets your needs.
The redaction feature does not meet the requirements for de-identification under medical privacy laws like the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), so we recommend you continue to treat it as protected health information after redaction.

For a list of the languages supported by Contact Lens redaction, see Languages supported by Amazon Connect.

**About redacted files**

Redacted voice files are stored in your Voice Amazon S3 bucket, for example: connect-\*instanceARN/Analysis.

Redacted chat files are stored in your chat Amazon S3 bucket, for example: connect-\*instanceARN/Chat

You can access all files (redacted, unredacted, raw, etc.) through the AWS console, by using the Amazon S3 console.

Following is a list of what you can access by using the Amazon Connect admin website (such as on the Contact details page), assuming you have the appropriate security profile permissions:

- Access redacted voice and chat files.
- Download redacted voice recordings.

**Note**

Currently, you cannot download redacted chat files and voice transcripts.

When redaction is enabled, Contact Lens generates the following files:

- A redacted file. This file is generated by default when Redaction is enabled. It's the output schema, with sensitive data redacted. For an example file, see Example redacted file for a call.
- An original (raw), analyzed file. This file is generated only when you choose Get redacted and original transcripts with redacted audio in the Set recording and analytics behavior block. For an example file, see Example original, analyzed file for a call.
Important

For voice contacts, the original analyzed file is the only place where the complete conversation is stored. If you delete it, there will be no record of the sensitive data that was redacted.

- A redacted audio file (wav) for voice contacts. Sensitive data in audio files is redacted as silence. These silent times are not flagged in the Amazon Connect admin website or elsewhere as non-talk time.

Use your file retention policies to determine how long to keep these files.

Use the API for real-time call and chat analytics

Contact Lens includes two APIs that support conversational analytics. Use these APIs to build solutions that make your contact center more efficient.

- **ListRealtimeContactAnalysisSegments**: Use for voice contacts.
- **ListRealtimeContactAnalysisSegmentsV2**: Use for chat contacts.

These real-time conversational analytics APIs are polling APIs, with a standard request/response exchange, where you don't need to integrate with any other service. However, there are rate limitations. If needed, you can eliminate these limitations by using the real-time streaming API. It requires integration with Amazon Kinesis Data Streams.

Following are two use cases for the real-time call and chat analytics API.

Better contact transfers

When a contact is transferred from one agent to another agent, you can transfer a transcript of the conversation to the new agent. The new agent then has context for why the customer is contacting your contact center, and the customer doesn't need to repeat information they already provided. Use the **ListRealtimeContactAnalysisSegments** API for voice contacts and the **ListRealtimeContactAnalysisSegmentsV2** API for chats to get the entire transcript of the conversation up to a certain point, and share it with the new agent.
Highlight key parts of the conversation as labels, issues, action items, and outcomes

With key highlights agents can quickly make notes after the contact ends, and supervisors can quickly identify contacts for quality and agent performance management. This makes agents and supervisors more productive at their jobs.

Use streaming for real-time contact analysis

Real-time contact analysis segment streams enable you to access Contact Lens analytics in near real-time. Real-time streaming overcomes the scaling limitations of existing real-time call analytics API. It also provides access to a data segment called Utterance that allows you to access partial transcripts. This enables you to meet ultra-low latency requirements to assist agents on live calls.

This section explains how to integrate with Amazon Kinesis Data Streams for real-time streaming.

Through real-time streaming, you can receive the following event types:

- STARTED events published at the beginning of a real-time contact analysis session.
- SEGMENTS events published during the real-time contact analysis sessions. These events contain a list of segments with analyzed information.
- COMPLETED or FAILED events published at the end of a real-time contact analysis session.

Contents

- Enable real-time contact analysis segment streams
- Real-time contact analysis segment streams data model
- Sample real-time contact analysis segment stream

Enable real-time contact analysis segment streams

Real-time contact analysis segment streams are not enabled by default. This topic explains how to enable them.

Step 1: Create a Kinesis stream

Create the data stream on the same account and Region where your Amazon Connect instance resides. For instructions, see Step 1: Create a Data Stream in the Amazon Kinesis Data Streams Developer Guide.
**Tip**

We recommend creating a separate stream for each type of data. While it's possible to use the same stream for real-time contact analysis segment streams, agent events, and contact records, it is much easier to manage and get data from the stream when you use a separate stream for each one. For more information, see the Amazon Kinesis Data Streams Developer Guide.

---

**Step 2: Set up server-side encryption for the Kinesis stream (optional but recommended)**

There are several ways you can do this.

- **Option 1:** Use the Kinesis AWS managed key (aws/kinesis). This works with no additional setup from you.

- **Option 2:** Use the same customer managed key for call recordings, chat transcripts, or exported reports in your Amazon Connect instance.

  Enable encryption, and use a customer managed key for call recordings, chat transcripts, or exported reports in your Amazon Connect instance. Then choose the same KMS key for your Kinesis data stream. This key already has the permission (grant) required to be used.

- **Option 3:** Use a different customer managed key.

  Use an existing customer managed key or create a new one and add required permissions for Amazon Connect role to use the key. To add permissions using AWS KMS grants, see the following example:

  ```bash
  aws kms create-grant \
  --key-id your key ID \
  --grantee-principal arn:aws:iam::your AWS account ID:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect_11111111111111111111 \
  --operations GenerateDataKey \
  --retiring-principal arn:aws:iam::your AWS account ID:role/adminRole
  ```

  Where grantee-principal is the ARN of the service-linked role associated to your Amazon Connect instance. To find the ARN of the service-linked role, in the Amazon Connect console, go to **Overview, Distribution settings, Service-linked role**.
**Step 3: Associate the Kinesis stream**

For voice contacts, use Amazon Connect `AssociateInstanceStorageConfig` API to associate the resource type `REAL_TIME_CONTACT_ANALYSIS_SEGMENTS` along with the Kinesis stream where real-time contact analysis segments will be published. You'll need the instance ID and the Kinesis stream ARN.

**AWS CLI**

```bash
aws connect associate-instance-storage-config --instance-id your Amazon Connect instance ID --resource-type REAL_TIME_CONTACT_ANALYSIS_SEGMENTS --storage-config 'StorageType=KINESIS_STREAM,KinesisStreamConfig={StreamArn=the ARN of your Kinesis stream}'
```

**AWS SDK**

```javascript
import { Connect } from 'aws-sdk';

async function associate (): Promise <void> {
    const clientConfig: Connect.ClientConfiguration = {
        region: 'the Region of your Amazon Connect instance',
    };

    const connect = new Connect(clientConfig);

    // Build request
    const request: Connect.Types.AssociateInstanceStorageConfigRequest = {
        InstanceId: 'your Amazon Connect instance ID',
        ResourceType: 'REAL_TIME_CONTACT_ANALYSIS_SEGMENTS',
        StorageConfig: {
            StorageType: 'KINESIS_STREAM',
            KinesisStreamConfig: {
                StreamArn: 'the ARN of your Kinesis stream',
            },
        },
    };

    try {
        // Execute request
        const response: Connect.Types.AssociateInstanceStorageConfigResponse = await connect.associateInstanceStorageConfig(request).promise();
    }
};
```
Step 4: Enable Contact Lens for your Amazon Connect instance

For instructions, see [Enable Amazon Connect Contact Lens](#).

Step 5 (Optional): Review a sample segment stream

We recommend you review a sample segment stream to familiarize yourself with what it looks like. See [Sample real-time contact analysis segment stream](#).

**Real-time contact analysis segment streams data model**

Real-time contact analysis segment streams are generated in JSON. Event JSON blobs are published to the associated stream for every contact that has real-time contact analysis enabled. The following types of events can be published for a real-time contact analysis session:

- **STARTED events**—Each real-time contact analysis session publishes one STARTED event at the beginning of the session.
- **SEGMENTS events**—Each real-time contact analysis session may publish zero or more SEGMENTS events during the session. These events contain a list of segments with analyzed information. The list of segments may include "Utterance," "Transcript," or "Categories" segments.
- **COMPLETED or FAILED events**—Each real-time contact analysis session publishes one COMPLETED or FAILED event at the end of the session.

**Common properties included in all events**

Every event includes the following properties:
Version

The version of the event schema.

Type: String

Channel

The type of channel for this contact.

Type: String

Valid values: VOICE, CHAT, TASK

For more information about channels, see Concepts: Channels and concurrency.

AccountId

The identifier of the account where this contact takes place.

Type: String

ContactId

The identifier of the contact being analyzed.

Type: String

InstanceId

The identifier of the instance where this contact takes place.

Type: String

LanguageCode

The language code associated to this contact.

Type: String

Valid values: the language code for one of the supported languages for Contact Lens real-time call analytics.

EventType

The type of event published.

Type: String
Valid values: STARTED, SEGMENTS, COMPLETED, FAILED

**STARTED event**

STARTED events include only the common properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: STARTED

**SEGMENTS event**

SEGMENTS events include the following properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: SEGMENTS
- Segments: In addition to the common properties, SEGMENTS events include a list of segments with analyzed information.

  Type: Array of Segment objects

**Segment**

An analyzed segment for a real-time analysis session.

Each segment is an object with the following optional properties. Only one of these properties is present, depending on the segment type:

- Utterance
Use streaming for real-time contact analysis
Type: Integer

**Transcript**

The analyzed transcript.

Type: Transcript object

Required: No

**Categories**

The matched category rules.

Type: Categories object

Required: No

**COMPLETED event**

COMPLETED events include only the following common properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: STARTED

**FAILED event**

FAILED events include only the following common properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: FAILED
Sample real-time contact analysis segment stream

This topic provides sample segment streams for STARTED, SEGMENTS, COMPLETED, and FAILED events.

Sample STARTED event

- **EventType: STARTED**
- Published at the beginning of the real-time contact analysis session.

```json
{
    "Version": "1.0.0",
    "Channel": "VOICE",
    "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "STARTED"
}
```

Sample SEGMENTS event

- **EventType: SEGMENTS**
- Published during a real-time contact analysis session. This event contains a list of segments with analyzed information. The list of segments may include "Utterance," "Transcript," or "Categories" segments.

```json
{
    "Version": "1.0.0",
    "Channel": "VOICE",
    "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "SEGMENTS",
    "Segments": [
        {
            "Utterance": {
                "Id": "the ID of the utterance",
                "TranscriptId": "the ID of the transcript",
            }
        }
    ]
}
```
"ParticipantId": "AGENT",
"ParticipantRole": "AGENT",
"PartialContent": "Hello, thank you for calling Example Corp. My name is Adam.",
"BeginOffsetMillis": 19010,
"EndOffsetMillis": 22980
}
",
{
"Utterance": {
"Id": "the ID of the utterance",
"TranscriptId": "the ID of the transcript",
"ParticipantId": "AGENT",
"ParticipantRole": "AGENT",
"PartialContent": "How can I help you?",
"BeginOffsetMillis": 23000,
"EndOffsetMillis": 24598
}
",
{
"Transcript": {
"Id": "the ID of the transcript",
"ParticipantId": "AGENT",
"ParticipantRole": "AGENT",
"Content": "Hello, thank you for calling Example Corp. My name is Adam. How can I help you?",
"BeginOffsetMillis": 19010,
"EndOffsetMillis": 24598,
"Sentiment": "NEUTRAL"
}
",
{
"Transcript": {
"Id": "the ID of the transcript",
"ParticipantId": "CUSTOMER",
"ParticipantRole": "CUSTOMER",
"Content": "I'm having trouble submitting the application, number AX876293 on the portal. I tried but couldn't connect to my POC on the portal. So, I'm calling on this toll free number",
"BeginOffsetMillis": 19010,
"EndOffsetMillis": 22690,
"Sentiment": "NEGATIVE",
"IssuesDetected": [ 

Sample COMPLETED event

- **EventType**: COMPLETED
- **Published at the end of the real-time contact analysis session if the analysis completed successfully.**
Sample FAILED event

- **EventType**: FAILED
- Published at the end of the real-time contact analysis session if the analysis failed.

Output file locations for files analyzed by Contact Lens

Following are examples of what the path looks like for Contact Lens output files when they are stored in the Amazon S3 bucket for your instance.

- Original analyzed transcript file (JSON)
  - /connect-instance- bucket/Analysis/
    - **Voice**: 2020/02/04/contact's_ID_analysis_2020-02-04T21:14:16Z.json
  - /connect-instance- bucket/Analysis/
    - **Chat**: 2020/02/04/contact's_ID_analysis_2020-02-04T21:14:16Z.json
- Redacted analyzed transcript file in (JSON)
  - /connect-instance- bucket/Analysis/Voice/
    - **Redacted**: 2020/02/04/contact's_ID_analysis_redacted_2020-02-04T21:14:16Z.json
• /connect-instance- bucket/Analysis/Chat/
  Redacted/2020/02/04/contact's_ID_analysis_redacted_2020-02-04T21:14:16Z.json

• Redacted audio file

• /connect-instance- bucket/Analysis/Voice/
  Redacted/2020/02/04/contact's_ID_call_recording_redacted_2020-02-04T21:14:16Z.wav

⚠️ Important
To delete a recording, you must delete the files for both the redacted and unredacted recordings.

Example Contact Lens output files for a call

Example original, analyzed file for a call

This section shows an example schema for a call that Contact Lens has analyzed. The example shows loudness, issue detection/call drivers, and what information is going to be redacted.

Note the following about the analyzed file:

• It doesn’t indicate what sensitive data was redacted. All data are referred to as PII (personally identifiable information).

• Each turn includes a Redaction section only if it includes PII.

• If a Redaction section exists, it includes the offset in milliseconds. In a .wav file, the redacted portion will be silence. If desired, you can use the offset to replace the silence with something else, such as a beep.

• If two or more PII redactions exist in a turn, the first offset applies to the first PII, the second offset applies to the second PII, and so on.

```json
{
  "Version": "1.1.0",
  "AccountId": "your AWS account ID",
  "Channel": "VOICE",
  "ContentMetadata": {
    "Output": "Raw"
  }
}
```
"JobStatus": "COMPLETED",
"LanguageCode": "en-US",
"Participants": [
  {
    "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
    "ParticipantRole": "CUSTOMER"
  },
  {
    "ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
    "ParticipantRole": "SYSTEM"
  },
  {
    "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
    "ParticipantRole": "AGENT"
  }
],
"Categories": {
  "MatchedCategories": [],
  "MatchedDetails": {}
},
"ConversationCharacteristics": {
  "TotalConversationDurationMillis": 32110,
  "Sentiment": {
    "OverallSentiment": {
      "AGENT": 0,
      "CUSTOMER": 3.1
    },
    "SentimentByPeriod": {
      "QUARTER": {
        "AGENT": [
          {
            "BeginOffsetMillis": 0,
            "EndOffsetMillis": 7427,
            "Score": 0
          },
          {
            "BeginOffsetMillis": 7427,
            "EndOffsetMillis": 14855,
            "Score": -5
          },
          {
            "BeginOffsetMillis": 14855,
            "EndOffsetMillis": 22282,
            "Score": 0
          }
        ]
      }
    }
  }
}
Call: Example Contact Lens output files
"AverageWordsPerMinute": 239
},
"CUSTOMER": {
  "AverageWordsPerMinute": 163
}
}
},
"TalkTime": {
  "TotalTimeMillis": 28698,
  "DetailsByParticipant": {
    "AGENT": {
      "TotalTimeMillis": 15079
    },
    "CUSTOMER": {
      "TotalTimeMillis": 13619
    }
  }
}
},
"CustomModels": [],
"Transcript": [
  {
    "BeginOffsetMillis": 0,
    "Content": "Okay.",
    "EndOffsetMillis": 90,
    "Id": "the ID of the turn",
    "ParticipantId": "AGENT",
    "Sentiment": "NEUTRAL",
    "LoudnessScore": [
      79.27
    ]
  },
  {
    "BeginOffsetMillis": 160,
    "Content": "Just hello. My name is Peter and help.",
    "EndOffsetMillis": 4640,
    "Id": "the ID of the turn",
    "ParticipantId": "CUSTOMER",
    "Sentiment": "NEUTRAL",
    "LoudnessScore": [
      66.56,
      40.06,
      85.27,
      82.22,
      ...
77.66
],
"Redaction": {
  "RedactedTimestamps": [
    {
      "BeginOffsetMillis": 3290,
      "EndOffsetMillis": 3620
    }
  ]
},
{
  "BeginOffsetMillis": 4640,
  "Content": "Hello. Peter, how can I help you?",
  "EndOffsetMillis": 6610,
  "Id": "the ID of the turn",
  "ParticipantId": "AGENT",
  "Sentiment": "NEUTRAL",
  "LoudnessScore": [
    70.23,
    73.05,
    71.8
  ],
  "Redaction": {
    "RedactedTimestamps": [
      {
        "BeginOffsetMillis": 5100,
        "EndOffsetMillis": 5450
      }
    ]
  }
},
{
  "BeginOffsetMillis": 7370,
  "Content": "I need to cancel. I want to cancel my plan subscription.",
  "EndOffsetMillis": 11190,
  "Id": "the ID of the turn",
  "ParticipantId": "CUSTOMER",
  "Sentiment": "NEGATIVE",
  "LoudnessScore": [
    77.18,
    79.59,
    85.23,
    81.08,
73.99
],
"IssuesDetected": [
{
    "CharacterOffsets": {
        "BeginOffsetChar": 0,
        "EndOffsetChar": 55
    },
    "Text": "I need to cancel. I want to cancel my plan subscription"
}
],
{
    "BeginOffsetMillis": 11220,
    "Content": "That sounds very bad. I can offer a 20% discount to make you stay with us."
},
    "EndOffsetMillis": 15210,
    "Id": "the ID of the turn",
    "ParticipantId": "AGENT",
    "Sentiment": "NEGATIVE",
    "LoudnessScore": [
        75.92,
        75.79,
        80.31,
        80.44,
        76.31
    ]
},
{
    "BeginOffsetMillis": 15840,
    "Content": "That sounds interesting. Thank you accept."
},
    "EndOffsetMillis": 18120,
    "Id": "the ID of the turn",
    "ParticipantId": "CUSTOMER",
    "Sentiment": "POSITIVE",
    "LoudnessScore": [
        73.77,
        79.17,
        77.97,
        79.29
    ]
},
{
    "BeginOffsetMillis": 18310,
"Content": "Alright, I made all the changes to the account and now these discounts applied.",
"EndOffsetMillis": 21820,
"Id": "the ID of the turn",
"ParticipantId": "AGENT",
"Sentiment": "NEUTRAL",
"LoudnessScore": [
  83.88,
  86.75,
  86.97,
  86.11
],
"OutcomesDetected": [
  {
    "CharacterOffsets": {
      "BeginOffsetChar": 9,
      "EndOffsetChar": 77
    },
    "Text": "I made all the changes to the account and now these discounts applied"
  }
],

"BeginOffsetMillis": 22610,
"Content": "Awesome. Thank you so much.",
"EndOffsetMillis": 24140,
"Id": "the ID of the turn",
"ParticipantId": "CUSTOMER",
"Sentiment": "POSITIVE",
"LoudnessScore": [
  79.11,
  81.7,
  78.15
],

"BeginOffsetMillis": 24120,
"Content": "No worries. I will send you all the details later today and call you back next week to check up on you.",
"EndOffsetMillis": 29710,
"Id": "the ID of the turn",
"ParticipantId": "AGENT",
"Sentiment": "POSITIVE",
"LoudnessScore": [ 
    87.07, 
    83.96, 
    76.38, 
    88.38, 
    87.69, 
    76.6 
], 
"ActionItemsDetected": [ 
    { 
        "CharacterOffsets": { 
            "BeginOffsetChar": 12, 
            "EndOffsetChar": 102 
        }, 
        "Text": "I will send you all the details later today and call you back next week to check up on you"
    } 
], 
}, 
{
    "BeginOffsetMillis": 30580, 
    "Content": "Thank you. Sir. Have a nice evening.", 
    "EndOffsetMillis": 32110, 
    "Id": "the ID of the turn", 
    "ParticipantId": "CUSTOMER", 
    "Sentiment": "POSITIVE", 
    "LoudnessScore": [ 
        81.42, 
        82.29, 
        73.29 
    ]
} 
] 
} 

Example redacted file for a call

This section shows an example redacted file for a call. It's a twin of the original analyzed file. The only difference is that sensitive data are redacted. In this example, three entities were selected for redaction: "CREDIT_DEBIT_NUMBER", "NAME", "USERNAME".
In this example, RedactionMaskMode is set to PII. When an entity is redacted, Contact Lens replaces it with `[PII]`. If it were set to ENTITY_TYPE, Contact Lens would replace the data with the name of the entity, for example, `[CREDIT_DEBIT_NUMBER]`.

```json
{
    "Version": "1.1.0",
    "AccountId": "your AWS account ID",
    "ContentMetadata": {
        "Output": "Redacted",
        "RedactionTypes": ["PII"],
        "RedactionTypesMetadata": {
            "PII": {
                "RedactionEntitiesRequested": ["CREDIT_DEBIT_NUMBER", "NAME", "USERNAME"],
                "RedactionMaskMode": "PII" // if you were to choose ENTITY_TYPE instead, the redaction would say, for example, [NAME]
            }
        }
    },
    "Channel": "VOICE",
    "JobStatus": "COMPLETED",
    "LanguageCode": "en-US",
    "Participants": [
        {
            "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
            "ParticipantRole": "CUSTOMER"
        },
        {
            "ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
            "ParticipantRole": "SYSTEM"
        },
        {
            "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
            "ParticipantRole": "AGENT"
        }
    ],
    "Categories": {
        "MatchedCategories": [],
        "MatchedDetails": {}
    },
    "ConversationCharacteristics": {
        "TotalConversationDurationMillis": 32110,
        "Sentiment": {
```
"OverallSentiment": {
   "AGENT": 0,
   "CUSTOMER": 3.1
  },
"SentimentByPeriod": {
   "QUARTER": {
     "AGENT": [
     {
      "BeginOffsetMillis": 0,
      "EndOffsetMillis": 7427,
      "Score": 0
     },
     {
      "BeginOffsetMillis": 7427,
      "EndOffsetMillis": 14855,
      "Score": -5
     },
     {
      "BeginOffsetMillis": 14855,
      "EndOffsetMillis": 22282,
      "Score": 0
     },
     {
      "BeginOffsetMillis": 22282,
      "EndOffsetMillis": 29710,
      "Score": 5
     }
    ],
   "CUSTOMER": [{
    "BeginOffsetMillis": 0,
    "EndOffsetMillis": 8027,
    "Score": -2.5
   },
   {
    "BeginOffsetMillis": 8027,
    "EndOffsetMillis": 16055,
    "Score": 5
   },
   {
    "BeginOffsetMillis": 16055,
    "EndOffsetMillis": 24082,
    "Score": 5
   },
   {
    "BeginOffsetMillis": 24082,
    "EndOffsetMillis": 32110,
    "Score": 5
   }]},
Call: Example Contact Lens output files

{  
  "BeginOffsetMillis": 24082,  
  "EndOffsetMillis": 32110,  
  "Score": 5  
}

"Interruptions": {  
  "InterruptionsByInterrupter": {},  
  "TotalCount": 0,  
  "TotalTimeMillis": 0  
},

"NonTalkTime": {  
  "TotalTimeMillis": 0,  
  "Instances": []  
},

"TalkSpeed": {  
  "DetailsByParticipant": {  
    "AGENT": {  
      "AverageWordsPerMinute": 239  
    },  
    "CUSTOMER": {  
      "AverageWordsPerMinute": 163  
    }  
  }  
},

"TalkTime": {  
  "TotalTimeMillis": 28698,  
  "DetailsByParticipant": {  
    "AGENT": {  
      "TotalTimeMillis": 15079  
    },  
    "CUSTOMER": {  
      "TotalTimeMillis": 13619  
    }  
  }  
},

"CustomModels": [],

"Transcript": [  
  {  
    "BeginOffsetMillis": 0,  
  }  
]
"Content": "Okay.",
"EndOffsetMillis": 90,
"Id": "the ID of the turn",
"ParticipantId": "AGENT",
"Sentiment": "NEUTRAL",
"LoudnessScore": [
  79.27
],
}
{
  "BeginOffsetMillis": 160,
  "Content": "Just hello. My name is [PII] and help.",
  "EndOffsetMillis": 4640,
  "Id": "the ID of the turn",
  "ParticipantId": "CUSTOMER",
  "Sentiment": "NEUTRAL",
  "LoudnessScore": [
    66.56,
    40.06,
    85.27,
    82.22,
    77.66
  ],
  "Redaction": {
    "RedactedTimestamps": [
      {
        "BeginOffsetMillis": 3290,
        "EndOffsetMillis": 3620
      }
    ]
  }
},
{
  "BeginOffsetMillis": 4640,
  "Content": "Hello. [PII], how can I help you?",
  "EndOffsetMillis": 6610,
  "Id": "the ID of the turn",
  "ParticipantId": "AGENT",
  "Sentiment": "NEUTRAL",
  "LoudnessScore": [
    70.23,
    73.05,
    71.8
  ],
"Redaction": {
   "RedactedTimestamps": [
      {
         "BeginOffsetMillis": 5100,
         "EndOffsetMillis": 5450
      }
   ]
},
{
   "BeginOffsetMillis": 7370,
   "Content": "I need to cancel. I want to cancel my plan subscription.",
   "EndOffsetMillis": 11190,
   "Id": "the ID of the turn",
   "ParticipantId": "CUSTOMER",
   "Sentiment": "NEGATIVE",
   "LoudnessScore": [
      77.18,
      79.59,
      85.23,
      81.08,
      73.99
   ],
   "IssuesDetected": [
      {
         "CharacterOffsets": {
            "BeginOffsetChar": 0,
            "EndOffsetChar": 55
         },
         "Text": "I need to cancel. I want to cancel my plan subscription"
      }
   ],
   "Sentiment": "NEGATIVE",
   "LoudnessScore": [
      75.92,
      75.79,
That sounds interesting. Thank you accept.

Alright, I made all the changes to the account and now these discounts applied.
Awesome. Thank you so much.

No worries. I will send you all the details later today and call you back next week to check up on you.

Thank you. Sir. Have a nice evening.
"Id": "the ID of the turn",
"ParticipantId": "CUSTOMER",
"Sentiment": "POSITIVE",
"LoudnessScore": [
    81.42,
    82.29,
    73.29
]
}
]

Example Contact Lens output files for a chat

This section shows an example schema for a chat conversation that Contact Lens has analyzed. The example shows inferred sentiment, matched categories, contact summary, and response time.

The original, analyzed file contains the full chat transcript. The same content that is present in the chat Transcript field on the Contact details page is present in Transcript field in the original Contact Lens analysis file. In addition, the analyzed file may contain more fields, such as a Redaction section to indicate that there is redacted data in the redacted analysis file.

⚠️ Note

Some ConversationCharacteristics include DetailsByParticipantRole maps, with participant roles as keys. However, not all roles from the Participants list (such as CUSTOMER or AGENT) are guaranteed to have corresponding keys in the DetailsByParticipantRole objects. The presence of a key for a participant depends on whether there was eligible data for ContactLens analysis.

Categories

PointsOfInterest differs between post-chat and post-call categories:

- Post-call PointsOfInterest has milliseconds offset.
- Post-chat PointsOfInterest has an array of TranscriptItems; each item has an id and CharacterOffset.
There is an array of PointsOfInterest. Each array has an array of TranscriptItems: each PointOfInterest is for a Category match, but each match can span across multiple transcript items.

For both calls and chats, the PointsOfInterest array can be empty. This means that the category is matched for the whole contact. For example, if you create a rule to match the category when Hello is not mentioned in the contact, there would be no portion of the transcript to pinpoint for this condition.

**Note**
Currently, category is inferred for text/plain, text/markdown chat messages only.

**Contact summary**

Contact summary is located in the ConversationCharacteristics.ContactSummary.SummaryItemsDetected array. No more than one item can be in that array, emphasizing that only one set of Issue, Outcome, and Action item can be found.

Each object in the array has following fields: IssuesDetected, OutcomesDetected, ActionItemsDetected.

Each of the fields has an array of TranscriptItems that has Id and CharacterOffsets. They describe TranscriptItems and specific parts that were identified to contain that contact summary: issue, outcome, or action item.

**Note**
Currently, contact summary is inferred for text/plain chat messages only.

**Sentiment**

**Overall sentiment**

The DetailsByParticipantRole field sentiment score for contact participants is similar to the Contact Lens for speech analytics file.
DetailsByInteraction field has CUSTOMER sentiment score for parts of chat interaction WithAgent and WithoutAgent. If there were no customer messages in those parts of interaction, the respective field will be absent.

Note
Currently, sentiment is inferred is for text/plain, text/markdown chat messages only.

Sentiment shift

The DetailsByParticipantRole field contains an object that describes the sentiment shift for contact participants (that is, AGENT, CUSTOMER): BeginScore and EndScore.

The DetailsByInteraction field has CUSTOMER sentiment shift for parts of the chat interaction WithAgent and WithoutAgent. If there were no customer messages in those parts of the interaction, the respective field will be absent.

Sentiment shift provides information about how the participant's sentiment changed throughout the chat interaction.

Response time

AgentGreetingTimeMillis measures the time between when the AGENT joined the chat and the moment when they ended their first message to customer.

DetailsByParticipantRole has following characteristics for each of participant:

• Average: What is average response time for a participant.
• Maximum: What is the longest response time for a participant. If there are multiple transcript items with the same maximum response time, which ones are they.

To calculate the Average and Maximum response times for a given participant, they need to respond to a message from another participant (AGENT needs to responds to the CUSTOMER, or vice versa).

For example, if there was only one message from CUSTOMER and then only one message from AGENT before the chat ended, Contact Lens will calculate a response time for the AGENT, but not for the CUSTOMER.
Note

Currently, response time is inferred is for text/plain, text/markdown chat messages only.

Redaction

Note the following about the original analysis file for chats:

- Transcript item includes a Redaction section only if it there is data to be redacted. The section contains character offsets for the data that is redacted in the redacted analysis file.
- If two or more pieces of a message are redacted, the first offset applies to the first redacted piece, the second offset applies to the second redacted piece, and so on.

DisplayNames for AGENT and CUSTOMER are redacted because they contain PII. This applies to AttachmentName, too.

CharacterOffsets take into consideration redaction changes of the Content length in the redacted analysis file. CharacterOffsets describe redacted content, not original content.

Example original chat file

```json
{
    "AccountId": "123456789012",
    "Categories": {
        "MatchedCategories": [
            "agent-intro"
        ],
        "MatchedDetails": {
            "agent-intro": {
                "PointsOfInterest": [
                    {
                        "TranscriptItems": [
                            {
                                "CharacterOffsets": {
                                    "BeginOffsetChar": 0,
                                    "EndOffsetChar": 73
                                },
                                "Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3d9a"
                            }
                        ]
                    }
                ]
            }
        }
    }
}
```
Chat: Example Contact Lens output files
"ResponseTime": {
    "AgentGreetingTimeMillis": 2511,
    "DetailsByParticipantRole": {
        "AGENT": {
            "Average": {
                "ValueMillis": 5575
            },
            "Maximum": {
                "TranscriptItems": [
                    {
                        "Id": "21acf0fc-7259-4a08-b4cd-688eb56587d3"
                    }
                ],
                "ValueMillis": 7309
            }
        },
        "CUSTOMER": {
            "Average": {
                "ValueMillis": 5875
            },
            "Maximum": {
                "TranscriptItems": [
                    {
                        "Id": "c71ad383-f876-4bb3-b254-7837b6a3d395"
                    }
                ],
                "ValueMillis": 11366
            }
        }
    },
    "Sentiment": {
        "DetailsByTranscriptItemGroup": [
            {
                "ParticipantRole": "AGENT",
                "ProgressiveScore": 0,
                "Sentiment": "NEUTRAL",
                "TranscriptItems": [
                    {
                        "Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3d9a"
                    }
                ]
            }
        ]
    }
}
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 1.6666666666666667,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    
  ]
},
"Sentiment": "POSITIVE",
"TranscriptItems": [
    {
        "Id": "21acf0fc-7259-4a08-b4cd-688eb56587d3"
    }
],
{
    "ParticipantRole": "AGENT",
    "ProgressiveScore": 1.6666666666666667,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
        {
            "Id": "2b8ba020-53ee-4053-b5b7-35364ac1c7df"
        }
    ]
},
{
    "ParticipantRole": "AGENT",
    "ProgressiveScore": 1.6666666666666667,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
        {
            "Id": "28d0a1ce-64d1-4625-bbef-4cfeb97b6742"
        }
    ]
},
{
    "ParticipantRole": "AGENT",
    "ProgressiveScore": 0,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
        {
            "Id": "ef9b8622-32d5-4cfd-9ccc-a242502267bc"
        },
        {
            "Id": "03a9de67-f9e1-4884-a1a3-ecea78a4ce9e"
        },
        {
            "Id": "cfee5ece-a671-4a11-9ec2-89aba4b7d688"
        }
    ]
}
"ParticipantRole": "AGENT",
"ProgressiveScore": 0,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
  "Id": "72cc8c8d-2199-422a-b363-01d6d3fd851"
}
],
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 1.6666666666666667,
  "Sentiment": "POSITIVE",
  "TranscriptItems": [
  {
    "Id": "61bb2591-fe87-44e4-bba0-a3619c4cef1f"
  }
  ],
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 1.6666666666666667,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
  {
    "Id": "1761f27e-0989-4b6d-a046-fc03d2c6bc9c"
  }
  ],
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 3.3333333333333335,
  "Sentiment": "POSITIVE",
  "TranscriptItems": [
  {
    "Id": "8cdff161-dc25-44e6-986f-fc0e08ee0a7d"
  }
  ],
},
{
  "ParticipantRole": "CUSTOMER",
  "ProgressiveScore": -1.6666666666666667,
  "Sentiment": "NEGATIVE",
  "TranscriptItems": [

Chat: Example Contact Lens output files
Chat: Example Contact Lens output files

```json
[
  {
    "ParticipantRole": "CUSTOMER",
    "ProgressiveScore": -3.75,
    "Sentiment": "NEGATIVE",
    "TranscriptItems": [
      {
        "Id": "7d5c07d7-3d26-4b34-ae91-39aeeaeef685c"
      },
      {
        "Id": "e0efbd17-9139-439b-8c80-ebf2b9b703b9"
      }
    ]
  },
  {
    "ParticipantRole": "CUSTOMER",
    "ProgressiveScore": -3.75,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
      {
        "Id": "8fbb8dd4-9fd4-4991-83dc-5f06eeead9aa"
      }
    ]
  },
  {
    "ParticipantRole": "CUSTOMER",
    "ProgressiveScore": -2.5,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
      {
        "Id": "3b856fd9-0eeb-4fb2-93ed-95ec4aae3a6"
      }
    ]
  },
  {
    "ParticipantRole": "CUSTOMER",
    "ProgressiveScore": 0,
    "Sentiment": "NEUTRAL",
    "TranscriptItems": [
      {
        "Id": "bcc51949-3a79-4398-be1b-a27345a8a8ad"
      }
    ]
  }
]
```
"Id": "ecb8c498-96d7-448b-8360-366e6edbb4090"
 ]
 },
 {
 "ParticipantRole": "CUSTOMER",
 "ProgressiveScore": 0,
 "Sentiment": "NEUTRAL",
 "TranscriptItems": [
  {
   "Id": "d334058f-e3de-4cf1-a3e1-32e46f1839"
  }
 ]
 },
 {
 "ParticipantRole": "CUSTOMER",
 "ProgressiveScore": 0,
 "Sentiment": "NEUTRAL",
 "TranscriptItems": [
  {
   "Id": "3ec6adb5-3f11-409c-af39-40cf7ba6f078"
  }
 ]
 },
 {
 "ParticipantRole": "CUSTOMER",
 "ProgressiveScore": 0,
 "Sentiment": "NEUTRAL",
 "TranscriptItems": [
  {
   "Id": "c71ad383-f876-4bb3-b254-7837b6a3d395"
  }
 ]
 },
 {
 "ParticipantRole": "CUSTOMER",
 "ProgressiveScore": 0,
 "Sentiment": "NEUTRAL",
 "TranscriptItems": [
  {
   "Id": "4b292b64-4a33-45ff-89df-d5a175d16d70"
  }
 ]
 },
},
Chat: Example Contact Lens output files
"CUSTOMER": {
    "WithAgent": 0
},
"DetailsByParticipantRole": {
    "AGENT": 1.1538461538461537,
    "CUSTOMER": 0
},
"SentimentShift": {
    "DetailsByInteraction": {
        "DetailsByParticipantRole": {
            "CUSTOMER": {
                "WithAgent": {
                    "BeginScore": -3,
                    "EndScore": 3.75
                }
            }
        },
        "DetailsByParticipantRole": {
            "AGENT": {
                "BeginScore": 0,
                "EndScore": 2.5
            },
            "CUSTOMER": {
                "BeginScore": -3.75,
                "EndScore": 3.75
            },
            "SYSTEM": {
                "BeginScore": 2.5,
                "EndScore": 0
            }
        }
    }
},
"CustomerMetadata": {
    "ContactId": "b49644f6-672f-445c-b209-f76b36482830",
    "InputS3Uri": "path to the json file in s3",
    "InstanceId": "f23fc323-3d6d-48aa-95dc-EXAMPLE012"
},
"JobStatus": "COMPLETED"
"LanguageCode": "en-US",
"Participants": [
{
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER"
},
{
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM"
},
{
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT"
}
],
"Transcript": [
{
"AbsoluteTime": "2022-10-27T03:31:50.735Z",
"ContentType": "application/vnd.amazonaws.connect.event.participant.joined",
"DisplayName": "John",
"Id": "740c494d-9df7-4400-91c0-3e4df33922c8",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "EVENT"
},
{
"AbsoluteTime": "2022-10-27T03:31:53.390Z",
"Content": "Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do.",
"ContentType": "text/plain",
"DisplayName": "SYSTEM_MESSAGE",
"Id": "78aa8229-714a-4c87-916b-ce7d8d567ab2",
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:31:55.131Z",
"Content": "The time in queue is less than 5 minutes.",
"ContentType": "text/plain",
"DisplayName": "SYSTEM_MESSAGE",
"Id": "1276382b-facb-49c5-8d34-62e3b0f50002",
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
}
]
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},

{
"AbsoluteTime": "2022-10-27T03:31:56.618Z",
"Content": "You are now being placed in queue to chat with an agent.",
"ContentType": "text/plain",
"DisplayName": "SYSTEM_MESSAGE",
"Id": "88c2363e-8206-4781-a353-c15e1ccacc12",
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},

{
"AbsoluteTime": "2022-10-27T03:32:00.951Z",
"ContentType": "application/vnd.amazonaws.connect.eventparticipant.joined",
"DisplayName": "Jane",
"Id": "c05cca74-d50b-4aa5-b46c-fdb5ae8c814c",
"ParticipantId": "f36a545d-67b2-4fd4-89eb-896136609a7",
"ParticipantRole": "AGENT",
"Type": "EVENT"
},

{
"AbsoluteTime": "2022-10-27T03:32:03.462Z",
"Content": "Hello, thanks for reaching Example Corp. This is Jane. How may I help you?",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3daa",
"ParticipantId": "f36a545d-67b2-4fd4-89eb-896136609a7",
"ParticipantRole": "AGENT",
"Redaction": {
"CharacterOffsets": [
{
"BeginOffsetChar": 46,
"EndOffsetChar": 53
}
],
"Type": "MESSAGE"
},

{
"AbsoluteTime": "2022-10-27T03:32:08.102Z",
"Message": "Chat: Example Contact Lens output files"
"Content": "I'd like to see if I can get a refund or an exchange, because I ordered one of your grow-it-yourself indoor herb garden kits and nothing sprouted after a couple weeks so I think something is wrong with the seeds and this product may be defective."

"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "bcc51949-3a79-4398-be1b-a27345a8a8ad",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
"Content": "My wife is blind and sensitive to the sun so I was going to surprise her for her birthday with all the herbs that she loves so you guys actually really let me down."

"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "7d5c07d7-3d26-4b34-ae91-39aeeef685c",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:18.781Z",
"Content": "I should be taking my business elsewhere. I don't see why I should be giving money to a company that isn't even going to sell a product that works."

"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "e0efbd17-9139-439b-8c80-ebf2b9b703b9",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:24.123Z",
"Content": "Ok. Can I get your first and last name please?"

"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "3673d926-6e75-4620-a6f0-7ea571790a15",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
Yeah. My first name is John and last name is Doe.

Could you please provide me with the order ID number?

Yes, just looking ...

Chat: Example Contact Lens output files
"AbsoluteTime": "2022-10-27T03:32:44.887Z",
"Content": "Not a problem, take your time.",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "3c4a2a1e-6790-46a6-8ad4-4a0980b04795",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:52.978Z",
"Content": "Okay, that should be #5376897. You know, if the product was fine I wouldn't have to scrounge through emails.",
"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "ecb8c498-96d7-448b-8360-366e69d4b90",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:59.441Z",
"Content": "alright, perfect. And could you also just confirm the shipping address for me?",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "f9cd41b6-3f68-4e83-a47d-664395f324c0",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Redaction": {
"CharacterOffsets": [
{
"BeginOffsetChar": 77,
"EndOffsetChar": 78
}
],
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:33:05.455Z",
"Content": "123 Any Street, Any Town, and the zip code is 98109."
"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "f9cd41b6-3f68-4e83-a47d-664395f324c0",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Redaction": {
"CharacterOffsets": [
{
"BeginOffsetChar": 77,
"EndOffsetChar": 78
}
],
"Type": "MESSAGE"
},
{
"Id": "d334058f-e3de-4cf1-a361-32e4e61f1839",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Redaction": {
  "CharacterOffsets": [
    {
      "BeginOffsetChar": 0,
      "EndOffsetChar": 27
    },
    {
      "BeginOffsetChar": 49,
      "EndOffsetChar": 54
    }
  ]
},
"Type": "MESSAGE"
},

"AbsoluteTime": "2022-10-27T03:33:12.764Z",
"Content": "Thank you very much. Just waiting on my system here. .. I'll also need the last four digits of your debit card.",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "21acf0fc-7259-4a08-b4cd-688eb56587d3",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
},

"AbsoluteTime": "2022-10-27T03:33:17.412Z",
"Content": "Ok. Last four for my debit care are 9008",
"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "3ec6adb5-3f11-409c-af39-40cf7ba6f078",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Redaction": {
  "CharacterOffsets": [
    {
      "BeginOffsetChar": 27,
      "EndOffsetChar": 31
    }
  ]
},
"AbsoluteTime": "2022-10-27T03:33:22.486Z",
"Content": "It's just too bad. I thought this was going to be the best gift idea. How can you guys be sending out defective seeds? Isn't that your whole business?",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "2b8ba020-53ee-4053-b5b7-35364ac1c7df",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b09a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:33:38.961Z",
"Content": "I apologize for the experience you had Mr. Doe, its very uncommon that our customer will have this issue. We will look into this and get this sorted out for you right away."
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "28d0a1ce-64d1-4625-bbef-4cfeb97b6742",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b09a7",
"ParticipantRole": "AGENT",
"Redaction": {
   "CharacterOffsets": [
      {
         "BeginOffsetChar": 41,
         "EndOffsetChar": 46
      }
   ]
},
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:33:44.192Z",
"Content": "Well, my wife's birthday already passed, so. There's not too much you can do. But I would still like to grow the herbs for her, if possible."
"ContentType": "text/markdown",
"DisplayName": "John",
"Id": "4b292b64-4a33-45ff-89df-d5a175d16d70",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfca",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"}
Totally understandable. Let me see what we can do for you. Please give me couple of minutes as I check the system.

Thank you sir one moment please.

Alright are you still there Mr Doe?

Yeah.
"DisplayName": "John",
"Id": "2da5a3c2-9d1b-458c-ae53-759a4e63198d",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
  "AbsoluteTime": "2022-10-27T03:34:12.562Z",
  "Content": "We are not only refunding the cost of the grow-it-yourself indoor herb kit but we will also be sending you a replacement. Would you be okay with this?",
  "ContentType": "text/markdown",
  "DisplayName": "Jane",
  "Id": "72cc8c8d-2199-422a-b363-01d6d3fdc851",
  "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
  "ParticipantRole": "AGENT",
  "Type": "MESSAGE"
},
{
  "AbsoluteTime": "2022-10-27T03:34:17.029Z",
  "Content": "Yeah! That would be great. I just want my wife to be able to have these herbs in her room. And I'm always happy to get my money back!",
  "ContentType": "text/markdown",
  "DisplayName": "John",
  "Id": "e23a2331-f3fc-4d3c-8a51-1541451186c9",
  "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
  "ParticipantRole": "CUSTOMER",
  "Type": "MESSAGE"
},
{
  "AbsoluteTime": "2022-10-27T03:34:22.269Z",
  "Content": "Awesome! We really want to keep our customers happy and satisfied, and again I want to apologize for your less than satisfactory experience with the last product you ordered from us."
  "ContentType": "text/markdown",
  "DisplayName": "Jane",
  "Id": "61bb2591-fe87-44e4-bba0-a3619c4cef1f",
  "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
  "ParticipantRole": "AGENT",
  "Type": "MESSAGE"
},
{
  "AbsoluteTime": "2022-10-27T03:34:26.353Z",
  "Content": "Okay! No problem. Sounds great. Thank you for all your help!",
  "ContentType": "text/markdown"
}
"Content": "Is there anything else I can help you out with John?",
"ContentType": "text/markdown",
"DisplayName": "Jane",
"Id": "1761f27e-0989-4b6d-a046-fc03d2c6bc9c",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Redaction": {
   "CharacterOffsets": [
      {
         "BeginOffsetChar": 48,
         "EndOffsetChar": 53
      }
   ]
},
"Type": "MESSAGE"
},
{
   "AbsoluteTime": "2022-10-27T03:34:36.704Z",
   "Content": "Nope!",
   "ContentType": "text/markdown",
   "DisplayName": "John",
   "Id": "540368c7-ec19-4fc0-8c86-0a5ee62d31a0",
   "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
   "ParticipantRole": "CUSTOMER",
   "Type": "MESSAGE"
},
{
   "AbsoluteTime": "2022-10-27T03:34:41.448Z",
   "Content": "Ok great! Have a great day.",
   "ContentType": "text/markdown",
   "DisplayName": "Jane",
   "Id": "8cdff161-dc25-44e6-986f-fc0e08ee0a7d",
   "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
   "ParticipantRole": "AGENT",
   "Type": "MESSAGE"
Example redacted chat file

```json
{
    "AccountId": "123456789012",
    "Categories": {
        "MatchedCategories": [
            "agent-intro"
        ],
        "MatchedDetails": {
            "agent-intro": {
                "PointsOfInterest": [
                    {
                        "TranscriptItems": [
                            {
                                "CharacterOffsets": {
                                    "BeginOffsetChar": 0,
                                    "EndOffsetChar": 71
                                },
                                "Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3d9a"
                            }
                        ]
                    }
                ]
            }
        }
    }
}
```
Chat: Example Contact Lens output files

1706
Chat: Example Contact Lens output files

Chat: Example Contact Lens output files
Chat: Example Contact Lens output files

```json
[
  {
    "Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3d9a"
  }
],
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "3673d926-6e75-4620-a6f0-7ea571790a15"
    }
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "46d37141-32d8-4f2e-a664-bcd3f34a68b3"
    }
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "3c4a2a1e-6790-46a6-8ad4-4a0980b04795"
    }
  ]
},
{
  "ParticipantRole": "AGENT",
  "ProgressiveScore": 0,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "f9cd41b6-3f68-4e83-a47d-664395f324c0"
    }
  ]
]
```
"ParticipantRole": "AGENT",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "POSITIVE",
"TranscriptItems": [
{
   "Id": "21acf0fc-7259-4a08-b4cd-688eb56587d3"
}
],
"ParticipantRole": "AGENT",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
   "Id": "2b8ba020-53ee-4053-b5b7-35364ac1c7df"
}
],
"ParticipantRole": "AGENT",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
   "Id": "28d0a1ce-64d1-4625-bbef-4cfeb97b6742"
}
],
"ParticipantRole": "AGENT",
"ProgressiveScore": 0,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
   "Id": "ef9b8622-32d5-4cfd-9ccc-a242502267bc"
},
{
   "Id": "03a9de67-f9e1-4884-a1a3-ecea78a4ce9e"
},
{
   "Id": "cfee5ece-a671-4a11-9ec2-89aba4b7d688"
"ParticipantRole": "AGENT",
"ProgressiveScore": 0,
"Sentiment": "NEUTRAL",
"TranscriptItems": [{
    "Id": "72cc8c8d-2199-422a-b363-01d6d3f8c851"
}]
},
{
"ParticipantRole": "AGENT",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "POSITIVE",
"TranscriptItems": [{
    "Id": "61bb2591-fe87-44e4-bba0-a3619c4cef1f"
}]
},
{
"ParticipantRole": "AGENT",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "NEUTRAL",
"TranscriptItems": [{
    "Id": "1761f27e-0989-4b6d-a046-fc03d2c6bc9c"
}]
},
{
"ParticipantRole": "AGENT",
"ProgressiveScore": 3.3333333333333335,
"Sentiment": "POSITIVE",
"TranscriptItems": [{
    "Id": "8c1d161-dc25-44e6-986f-fc0e08ee0a7d"
}]
}
"ParticipantRole": "CUSTOMER",
"ProgressiveScore": -1.6666666666666667,
"Sentiment": "NEGATIVE",
"TranscriptItems": [
  {
    "Id": "bcc51949-3a79-4398-be1b-a27345a8a8ad"
  }
],
{
  "ParticipantRole": "CUSTOMER",
  "ProgressiveScore": -3.75,
  "Sentiment": "NEGATIVE",
  "TranscriptItems": [
    {
      "Id": "7d5c07d7-3d26-4b34-ae91-39aeaeef685c"
    },
    {
      "Id": "e0efbd17-9139-439b-8c80-ebf2b9b703b9"
    }
  ]
},
{
  "ParticipantRole": "CUSTOMER",
  "ProgressiveScore": -3.75,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "8fbb8dd4-9fd4-4991-83dc-5f06eeead9aa"
    }
  ]
},
{
  "ParticipantRole": "CUSTOMER",
  "ProgressiveScore": -2.5,
  "Sentiment": "NEUTRAL",
  "TranscriptItems": [
    {
      "Id": "3b856fd9-0eeb-4fb2-93ed-95ec4aeae3a6"
    }
  ]
},
{
  "ParticipantRole": "CUSTOMER",
  "ProgressiveScore": -1.6666666666666667,
  "Sentiment": "NEGATIVE",
  "TranscriptItems": [
    {
      "Id": "bcc51949-3a79-4398-be1b-a27345a8a8ad"
    }
  ]
}
Chat: Example Contact Lens output files
"Id": "4b292b64-4a33-45ff-89df-d5a175d16d70"
}
],
{
"ParticipantRole": "CUSTOMER",
"ProgressiveScore": 0,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
"Id": "2da5a3c2-9d1b-458c-ae53-759a4e63198d"
}
],
{
"ParticipantRole": "CUSTOMER",
"ProgressiveScore": 1.6666666666666667,
"Sentiment": "POSITIVE",
"TranscriptItems": [
{
"Id": "e23a2331-f3fc-4d3c-8a51-1541451186c9"
}
],
{
"ParticipantRole": "CUSTOMER",
"ProgressiveScore": 3.75,
"Sentiment": "POSITIVE",
"TranscriptItems": [
{
"Id": "5a27cc39-9b73-4ebe-9275-5e6723788a1b"
}
],
{
"ParticipantRole": "CUSTOMER",
"ProgressiveScore": 3.75,
"Sentiment": "NEUTRAL",
"TranscriptItems": [
{
"Id": "540368c7-ec19-4fc0-8c86-0a5ee62d31a0"
}
]
"OverallSentiment": {
   "DetailsByInteraction": {
      "DetailsByParticipantRole": {
         "CUSTOMER": {
            "WithAgent": 0
         }
      }
   },
   "DetailsByParticipantRole": {
      "AGENT": 1.1538461538461537,
      "CUSTOMER": 0
   }
   },
   "SentimentShift": {
      "DetailsByInteraction": {
         "DetailsByParticipantRole": {
            "CUSTOMER": {
               "WithAgent": {
                  "BeginScore": -3,
                  "EndScore": 3.75
               }
            }
         }
      },
      "DetailsByParticipantRole": {
         "AGENT": {
            "BeginScore": 0,
            "EndScore": 2.5
         },
         "CUSTOMER": {
            "BeginScore": -3.75,
            "EndScore": 3.75
         }
      }
   }
},
"CustomerMetadata": {
   "ContactId": "b49644f6-672f-445c-b209-f76b36482830",
   "InputS3Uri": "path to the json file in s3",
   "InstanceId": "f23fc323-3d6d-48aa-EXAMPLE012"
},
"JobStatus": "COMPLETED",}
"LanguageCode": "en-US",
"Participants": [
    {
      "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
      "ParticipantRole": "CUSTOMER"
    },
    {
      "ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
      "ParticipantRole": "SYSTEM"
    },
    {
      "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
      "ParticipantRole": "AGENT"
    }
],
"Transcript": [
    {
      "AbsoluteTime": "2022-10-27T03:31:50.735Z",
      "ContentType": "application/vnd.amazonaws.connect.event.participant.joined",
      "DisplayName": "[PII]",
      "Id": "740c494d-9df7-4400-91c0-3e4df33922c8",
      "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
      "ParticipantRole": "CUSTOMER",
      "Type": "EVENT"
    },
    {
      "AbsoluteTime": "2022-10-27T03:31:53.390Z",
      "Content": "Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do."
    },
    {
      "AbsoluteTime": "2022-10-27T03:31:55.131Z",
      "Content": "The time in queue is less than 5 minutes."
    }
]
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:31:56.618Z",
"Content": "You are now being placed in queue to chat with an agent.",
"ContentType": "text/plain",
"DisplayName": "SYSTEM_MESSAGE",
"Id": "88c2363e-8206-4781-a353-c15e1ccacc12",
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:00.951Z",
"ContentType": "application/vnd.amazonaws.connect.event.participant.joined",
"DisplayName": "[PII]",
"Id": "c05cca74-d50b-4aa5-b46c-fdb5ae8c814c",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "EVENT"
},
{
"AbsoluteTime": "2022-10-27T03:32:03.462Z",
"Content": "Hello, thanks for reaching Example Corp. This is [PII]. How may I help you?",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "e4949dd1-aaa1-4fbd-84e7-65c95b2d3d9a",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Redaction": {
"CharacterOffsets": [
{
"BeginOffsetChar": 46,
"EndOffsetChar": 51
}
]
},
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:08.102Z",
"Content": "You are now being placed in queue to chat with an agent.",
"ContentType": "text/plain",
"DisplayName": "SYSTEM_MESSAGE",
"Id": "88c2363e-8206-4781-a353-c15e1ccacc12",
"ParticipantId": "2b2288b4-ff6e-4996-8d8e-260fd5a8ac02",
"ParticipantRole": "SYSTEM",
"Type": "MESSAGE"
},

"Content": "I'd like to see if I can get a refund or an exchange, because I ordered one of your grow-it-yourself indoor herb garden kits and nothing sprouted after a couple weeks so I think something is wrong with the seeds and this product may be defective."

"Content": "My wife is blind and sensitive to the sun so I was going to surprise her for her birthday with all the herbs that she loves so you guys actually really let me down."

"Content": "I should be taking my business elsewhere. I don't see why I should be giving money to a company that isn't even going to sell a product that works."

"Content": "Ok. Can I get your first and last name please?"
"AbsoluteTime": "2022-10-27T03:32:29.879Z",
"Content": "Yeah. My first name is [PII] and last name [PII].",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "8fbb8dd4-9fd4-4991-83dc-5f06eeead9aa",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Redaction": {
  "CharacterOffsets": [
  {
    "BeginOffsetChar": 21,
    "EndOffsetChar": 26
  },
  {
    "BeginOffsetChar": 44,
    "EndOffsetChar": 49
  }
]
},
"Type": "MESSAGE"
},
"AbsoluteTime": "2022-10-27T03:32:34.670Z",
"Content": "Could you please provide me with the order ID number?",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "46d37141-32d8-4f2e-a664-bcd3f34a68b3",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
},
"AbsoluteTime": "2022-10-27T03:32:39.726Z",
"Content": "Yes, just . Looking ...",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "3b856fd9-0ebeb-4fb2-93ed-95ec4aeae3a6",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
"AbsoluteTime": "2022-10-27T03:32:44.887Z",
"Content": "Not a problem, take your time.",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "3c4a2a1e-6790-46a6-8ad4-4a0980b04795",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:52.978Z",
"Content": "Okay, that should be #5376897. You know, if the product was fine I wouldn't have to scrounge through emails.",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "ecb8c498-96d7-448b-8360-366eeddb4090",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:32:59.441Z",
"Content": "Alright, perfect. And could you also just confirm the shipping address for me, [PII]",
"ContentType": "text/plain",
"DisplayName": "[PII]",
"Id": "f9cd41b6-3f68-4e83-a47d-664395f324c0",
"ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
"ParticipantRole": "AGENT",
"Redaction": {
   "CharacterOffsets": [
      {
         "BeginOffsetChar": 77,
         "EndOffsetChar": 82
      }
   ]
},
"Type": "MESSAGE"
},
{
"AbsoluteTime": "2022-10-27T03:33:05.455Z",
"Content": "[PII], and the zip code [PII].",
"ContentType": "text/plain",
"DisplayName": "[PII]",}
"Id": "d334058f-e3de-4cf1-a361-32e4e61f1839",
"ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
"ParticipantRole": "CUSTOMER",
"Redaction": {
   "CharacterOffsets": [
      {
         "BeginOffsetChar": 0,
         "EndOffsetChar": 5
      },
      {
         "BeginOffsetChar": 27,
         "EndOffsetChar": 32
      }
   ]
},
"Type": "MESSAGE"
},
{
   "AbsoluteTime": "2022-10-27T03:33:12.764Z",
   "Content": "Thank you very much. Just waiting on my system here. .. I'll also need the last four digits of your debit card.",
   "ContentType": "text/plain",
   "DisplayName": "[PII]",
   "Id": "21acf0fc-7259-4a08-b4cd-688eb56587d3",
   "ParticipantId": "f36a545d-67b2-4fd4-89fb-896136b609a7",
   "ParticipantRole": "AGENT",
   "Type": "MESSAGE"
},
{
   "AbsoluteTime": "2022-10-27T03:33:17.412Z",
   "Content": "Ok. Last four for my debit card [PII]",
   "ContentType": "text/plain",
   "DisplayName": "[PII]",
   "Id": "3ec6adb5-3f11-409c-af39-40cf7ba6f078",
   "ParticipantId": "e9b36a6d-12aa-4c21-9745-1881648ecfc8",
   "ParticipantRole": "CUSTOMER",
   "Redaction": {
      "CharacterOffsets": [
         {
            "BeginOffsetChar": 27,
            "EndOffsetChar": 32
         }
      ]
   }
},
It's just too bad. I thought this was going to be the best gift idea. How can you guys be sending out defective seeds? Isn't that your whole business?,

I apologize for the experience you had Mr [PII], its very uncommon that our customer will have this issue. We will look into this and get this sorted out for you right away.

Well, my wife's birthday already passed, so. There's not too much you can do. But I would still like to grow the herbs for her, if possible.
Totally understandable. Let me see what we can do for you. Please give me couple of minutes as I check the system.

Thank you sir one moment please.

Alright are you still there Mr [PII]?

Yeah.
We are not only refunding the cost of the grow-it-yourself indoor herb kit but we will also be sending you a replacement. Would you be okay with this?,

Yeah! That would be great. I just want my wife to be able to have these herbs in her room. And I'm always happy to get my money back!,

Awesome! We really want to keep our customers happy and satisfied, and again I want to apologize for your less than satisfactory experience with the last product you ordered from us.

Okay! No problem. Sounds great. Thank you for all your help!
Is there anything else I can help you out with Mr [PII]?

Nope!

Ok great! Have a great day.
Troubleshoot issues in Contact Lens

Why don't I see color-coded bars on my Amazon Connect admin website?

If your Amazon Connect admin website doesn't include color-coded bars similar to those shown in the preceding image, check whether the conversation that you're trying to analyzed occurred before June 30, 2020.

This view of conversations works only if the Contact Lens is enabled, and then the conversation occurred after June 30, 2020. This is because the feature that displays analyzed conversations in this format was released on June 30, 2020, and it can only be applied to conversations that happen after that time.

Why don't I see or hear unredacted content?

If your organization is using the Contact Lens redaction feature, by default only redacted content appears in the Amazon Connect admin website.

You must have permissions to view unredacted content. For more information, see Security profile permissions for Contact Lens.
Evaluate agent performance

Amazon Connect helps you to assess, track, and improve how agents interact with customers and resolve issues. For example, you can search for a contact, choose the appropriate evaluation form, review the contact audio, transcript, or both, and then evaluate how the agent interacted with the customer. You can then use that feedback to help the agent deliver improved customer experiences.

Tip

IT administrators: To enable Amazon Connect evaluation capabilities, go to the Amazon Connect console, choose your instance alias, choose Data storage, Content evaluations, Edit. You'll be prompted to create or choose an S3 bucket. After the bucket is created, you can store evaluations and export them.

To evaluate performance

1. Log in to Amazon Connect with a user account that has permissions to perform evaluations.

2. Access the contact that you want to evaluate. There are a few ways you can do this. For example, someone may have shared the contact URL with you, or assigned you a task that has the URL. Or, you may have the contact ID, which lets you search for the contact record by doing the following: on the navigation pane, choose Analytics and optimization, Contact search, and then search for the contact that you want to evaluate.

3. On the Contact details page, choose Evaluations or the < icon.

4. The Evaluations pane lists any evaluations that are in progress or completed for the contact.
To start an evaluation, choose an evaluation from the dropdown menu, and then choose *Start evaluation.*

To navigate an especially long evaluation form, use the arrows next to each section to collapse or expand it.

Choose *Save* to save a form in progress. The status of the form becomes *Draft.* You can return to it any time to continue, or you can delete it and start over.
When you're done, choose **Submit**. The status of the form is **Completed**.

### Create an evaluation form

In Amazon Connect, you can create *many different evaluation forms*. For example, you may need a different evaluation form for each business unit and type of interaction. Each form can contain multiple sections and questions. You can assign **weights** to each question and section to indicate how much their score impacts the agent's total score.

This topic explains how to create a form using the Amazon Connect admin website. To create and manage forms programmatically, see the [Evaluation actions](#) in the *Amazon Connect API Reference*.

**Contents**

- **Step 1**: Assign a title to the form
- **Step 2**: Add sections and questions
- **Step 3**: Add answers
- **Step 4**: Assign scores and ranges to answers
- **Step 5**: Enable automated evaluations
- **Step 6**: Preview the evaluation form
- **Step 7**: Assign weights for final score
- **Step 8**: Activate an evaluation form
**Step 1: Assign a title to the form**

In this step, you assign a title to the form. Evaluators will see this title in a dropdown menu.

1. Log in to Amazon Connect with a user account that has **permissions to create evaluation forms**.
2. In Amazon Connect, choose **Analytics and optimization, Evaluation forms**.
3. On the **Evaluation forms** page, choose **Create new form**.
4. Assign a title for the form, for example, **Sales evaluation**. Choose **Ok**.

5. At the top of the evaluation form page, there are two tabs:
   - **Sections and questions**. Add sections, questions, and answers to the form.
   - **Scoring**. Enable scoring on the form. You can also apply scoring to sections or questions.
6. Choose **Save** at any time while creating your form. This enables you to navigate away from the page and return to the form later.

7. Continue to the next step to add sections and questions.

**Step 2: Add sections and questions**

1. While on the **Sections and questions** tab, add a title to the section 1, for example, **Greeting**.

   ![Sales evaluation section](image)

   - **Section title**: Greeting
   - **Instructions to evaluators** — optional

2. Choose **Add question** to add a question.

3. In the **Question title** box, enter the question that will appear on the evaluation form. For example, **Did the agent state their name and say they are here to assist?**

   ![Sales evaluation question](image)

   - **Question title**: Did the agent state their name and say they are here to assist?
   - **Question type**: Single selection

4. In the **Instructions to evaluators** box, add information to help the evaluators answer the question, such as a link to an internal wiki or other resource.
5. In the **Question type** box, choose one of the following options to appear on the form:

- **Single selection**: The evaluator can choose from a list of options, such as **Yes**, **No**, or **Good**, **Fair**, **Poor**.
- **Text field**: The evaluator can enter free form text.
- **Number**: The evaluator can enter a number from a range that you specify, such as 1-10.

6. Continue to the next step to add answers.

**Step 3: Add answers**

1. On the **Answers** tab, add answer options that you want to display to evaluators, such as **Yes**, **No**.

2. To add more answers, choose **Add option**.

The following image shows example answers for a **Single selection** question.

The following image shows an answer range for a **Number** question.
3. When you're finished adding answers, continue to the next step to enable scoring, and add ranges for scoring **Number** answers.

**Step 4: Assign scores and ranges to answers**

1. Go to the top of the form. Choose the **Scoring** tab, and then choose **Enable scoring**.

   ![Enable scoring](image)

   This enables scoring for the entire form. It also enables you to add ranges for answers to **Number** question types.

2. Return to the **Sections and questions** tab. Now you have the option to assign scores to **Single selection**, and add ranges for **Number** question types.
3. When you create a **Number** type question, on the **Scoring** tab, choose **Add range** to enter a range of values. Indicate the worst to best score for the answer.

The following image shows an example of ranges and scoring for a **Number** question type.

- If the agent interrupted the customer 0 times, they get a score of 10 (best).
• If the agent interrupted the customer 1-4 times, they get a score of 5.
• If the agent interrupted the customer 5-10 times, they get a score of 1 (worst).

⚠️ Important
If you assign a score of **Automatic fail** to a question, *the entire evaluation form is assigned a score of 0*. The **Automatic fail** option is shown in the following image.

4. After you assign scores to all the answers, choose **Save**.
5. When you're finished assigning scores, continue to the next step to automate the question of certain questions, or continue to [preview the evaluation form](#).

### Step 5: Enable automated evaluations

Contact Lens lets you to define agent performance criteria (for example, adherence to required scripts), and then use that criteria to automatically complete evaluation forms. You set up the criteria and logic for each question where you want to allow automated evaluations.

Following are examples of setting up automated evaluations, one for a Single section question and another for a Numeric question.

#### Example automation for a Single selection question

• If the agent mentioned X or Y in the script, score this question as Yes.
The following image shows that when Contact Lens detects the words or phrases in the **ScriptCompliance** category, the question will automatically be answered **Yes**.

For information about setting up the criteria, see [Automatically categorize contacts based on keywords and phrases used during a conversation](#).

**Example automation for a Numeric question**

- If the agent interaction duration was less than 30 seconds, score the question as a 10.

- On the **Automation** tab, choose the metric that is used to automatically evaluate the question.
You can use any metadata that is a number. For example, first response time, sentiment score, and non-talk time.

Step 6: Preview the evaluation form

The Preview button is active only after you have assigned scores to answers for all of the questions.

The following image shows the form preview. Use the arrows to collapse sections and make the form easier to preview. You can edit the form while viewing the preview, as shown in the following image.
Step 7: Assign weights for final score

When scoring is enabled for the evaluation form, you can assign weights to sections or questions. The weight raises or lowers the impact of a section or question on the final score of the evaluation.

Weight distribution mode

With Weight distribution mode, you choose whether to assign weight by section or question:
- **Weight by section**: You can evenly distribute the weight of each question in the section.

- **Weight by question**: You can lower or raise the weight of specific questions.

When you change a weight of a section or question, the other weights are automatically adjusted so the total is always 100 percent.

For example, in the following image, three of the questions were manually set to 10 percent. The weights that display in italics were adjusted automatically.

---

**Example Evaluation Form**

![Example Evaluation Form](image)

The weight for sections cannot be changed manually when in **Questions** distribution mode.

- **Reset weight to default value**

- **Italics indicates the weight is automatically calculated**

---

**Step 8: Activate an evaluation form**

Choose **Activate** to make the form available to evaluators. Evaluators will no longer be able to choose the previous version of the form from the dropdown list.

Previous versions of the form are linked to the completed evaluations based on them. This allows you to view the version of the form that the evaluation is based on.

**View an evaluation form audit trail**

1. Select the evaluation form that you want to research.
2. At the bottom of the page, under **Example Evaluation**, use the dropdown menu to view previous versions, who accessed them, and when. The following image shows an example audit trail.

3. Optionally, choose one of the forms to open it.

**What do Active, Draft, and Locked mean?**

An form is in one of the following states:

- **Active**. A published version of the form that is available to evaluators.
- **Draft**. An inactive, locked version of the form. A draft is unlocked only when you are working on it.
- **Locked**. An evaluation form is locked when you activate or publish it. Even after you deactivate the form, it stays locked, and becomes a historical version of the form. However, you can activate the historical version to save it as new version.

**How scoring and weights work on evaluation forms**

By using **weights**, you can increase or decrease the impact of a question or section score on the overall evaluation score.
When scoring is enabled for the evaluation form, you can assign *weights* to sections or questions. The weight raises or lowers the impact of a section or question on the final score of the evaluation.

**Example score**

Let's say you are assigning the score to a question is that critically important to your business. If the answer is a Yes, the agent gets 10 points. For No they get 0 points. This is shown in the following image.

The answer to first question is more important to your business than the answer to *Did the agent close with “Is there anything else I can assist you with today?”*, which is also worth 0-10 points, as shown in the following image.

To differentiate scores of the questions, you indicate that weight of one question is more than the other.
The following image shows that the answer to *Did the agent recite the compliance script for the medication* is 50% of the agent's score. Whereas the answer to *Did the agent close with "Is there anything else I can assist you with today"* weighs only 5% of the score.

The total weight must always equal 100%.

**Weight distribution mode**

With **Weight distribution mode**, you choose whether to assign weight by section or question:

- **Weight by section:** You can evenly distribute the weight of each question in the section.
- **Weight by question:** You can lower or raise the weight of specific questions.

When you change a weight of a section or question, the other weights are automatically adjusted so the total is always 100 percent.

For example, in the following image, three of the questions were manually set to 10 percent. The weights that display in italics were adjusted automatically.
Create supervisor alerts on agent performance

You can create rules that automatically send emails or tasks to supervisors based on evaluation results. This feature helps facilitate quality assurance audits, enabling supervisors to thoroughly review evaluation results.

For example, you may want supervisors to review any evaluation forms that have an answer that is a compliance risk for your company.

Contents

- **Step 1: Define rule conditions**
- **Step 2: Define rule actions**
- **Example rule with multiple conditions**

**Step 1: Define rule conditions**

1. On the navigation menu, choose **Analytics and optimization, Rules**.
2. Select **Create a rule, Evaluation forms**.
3. Under **When**, use the dropdown list to choose **A Contact Lens evaluation result is available**, as shown in the following image.

![Rules editor](image)

4. Choose **Add condition**.

![Rules editor](image)

You can combine criteria from a set of conditions to build very specific Contact Lens rules. Following are the available conditions:

- **Evaluation - Form score**: Build rules that run when the score for a specific evaluation form is met.
- **Evaluation - Section score**: Build rules that run when the score for a specific section is met.
• **Evaluation - Question answer**: Build rules that run when the score for a specific question and answer is met.

• **Evaluation - Results available**: Build rules that run on any evaluation submissions.

• **Agent**: Build rules that run on a subset of agents. For example, create a rule to ensure newly hired agents comply with company standards.

  To see agent names so you can add them to rules, you need **Users - View** permissions in your security profile.

• **Queues**: Build rules that run on a subset of queues. Often organizations use queues to indicate a line of business, topic, or domain. For example, you could build rules specifically for the evaluations of those agents assigned to sales queues.

  To see the queue names so you can add them to rules, you need **Queues - View** permissions in your security profile.

• **Contact attributes**: Build rules that run on the values of custom **contact attributes**. For example, you can build rules for agent evaluations for a particular line of business or for specific customers, such as based on their membership level, their current country of residence, or if they have an outstanding order.

5. Choose **Next**.

**Step 2: Define rule actions**

1. Choose **Add action**. You can choose the following actions:

   • **Create Task**
   
   • **Send email notification**
   
   • **Generate an EventBridge event**
2. Choose **Next**.

3. Review and make any edits, then choose **Save**.

4. After you add rules, they are applied to new evaluation submissions that occur after the rule was added. You cannot apply rules to past, stored evaluations.

**Example rule with multiple conditions**

The following image shows a sample rule with six conditions. If any of these conditions are met, the action is triggered.
1. **Evaluation - Form score**: Does the Compliance Form have a score greater than or equal to 50%?

2. **Evaluation - Section score**: In a Compliance Form, does the Greeting section have a score greater than or equal to 70%?

3. **Evaluation - Question score**: Does the Compliance Form question *Did the agent greet the customer properly* equal Yes?

4. **Evaluation - Results available**: Have any results been generated for the Compliance Form?

5. **Queues**: Is this for the BasicQueue?

6. **Contact attributes**: Does CustomerType equal VIP?

**Search evaluation forms, scores, status, and evaluator**

1. Log in to Amazon Connect with a user account that has permissions to access contact records and the Evaluation forms - perform evaluations permission.

2. In Amazon Connect choose Analytics and optimization, Contact search.

3. Use the filters on the page to narrow your search. For date, you can search up to 8 weeks at a time.
Use reference ID for questions

A *reference ID* is a token that appears in the JSON output file. It represents a specific question. When building reports, you can use it in place of the exact wording of a question.

For example, a question might be "Did agents stick to the script?" but the next day the question might be changed to "Was there good script adherence?" Regardless of how the question is worded, the reference ID always stays the same.

**Example evaluation form output**

This section shows the export output path for evaluations, and provides an example of evaluation form scores and metadata.

**Verify your S3 bucket**

When you enable **Contact evaluations** in the Amazon Connect console, you are prompted to create or choose an S3 bucket to store the evaluations. To verify the name of the bucket, go to your instance alias, choose **Data storage, Contact evaluations, Edit**.

**Example output locations**

Following is the output file path for evaluation forms:

- `contact_evaluations_S3_bucket/Evaluations/YYYY/MM/DD/hh:mm:ss.sTZD-evaluation_id.json`
For example:

amazon-connect-s3/
Evaluations/2022/04/14/05:04:20.869Z-11111111-2222-3333-4444-555555555555.json

**Known issue: Two output files for the same evaluation**

Contact Lens generates two output files for the same evaluation form.

- One file is written to the new default S3 path. You can configure the path in the AWS console.
- Another file, which will be deprecated, is written to a different, previous S3 path. You can disregard this file.

The previous S3 path looks like the following:

- `s3_bucket/Evaluations/contact_contactId/evaluation_evaluationId/YYYY-MM-DDThh:mm:ss.sTZD.json`

**Example scores and metadata**

```json
{
    "schemaVersion": "3.1",
    "evaluationId": "fb90de35-4507-479a-8b57-970290fd5c2c",
    "metadata": {
        "contactId": "badd4896-75f7-43b3-bee6-c617ed3d04cb",
        "accountId": "874551140838",
        "instanceId": "8f753c94-9cd2-4f16-85eb-945f7f0d559a",
        "agentId": "286bcec0-e722-4166-865f-84db80252218",
        "evaluationDefinitionTitle": "Compliance Evaluation Form",
        "evaluator": "jane",
        "evaluationDefinitionId": "15d8fbf1-b4b2-4ace-869b-82714e2f6e3e",
        "evaluationDefinitionVersion": 2,
        "evaluationStartTimestamp": "2022-11-14T17:57:08.649Z",
        "evaluationSubmitTimestamp": "2022-11-14T17:59:29.052Z",
        "score": { "percentage": 100 }
    },
    "sections": [
        {
            "sectionRefId": "s1a1b58d6",
            "sectionTitle": "The title of the section",
            "notes": "Section note",
            "score": { "percentage": 100 }
        }
    ]
}
```

Example evaluation form output
The title of the subsection

1. How do you rate the contact between 1 and 10?
   - Answer: Add more information here
   - Notes: Add more information here
   - Score: notApplicable: true

2. Did the agent introduce themselves?
   - Values: Yes, No, Maybe
   - Notes: Add more information here
   - Metadata: notApplicable: false
   - Score: percentage: 100

3. Describe the outcome.
   - Value: Example answer text
Assign security profile permissions for evaluation forms

To allow users to create, define, and access evaluation forms, assign the following **Analytics and optimization** security profile permissions:

- **Evaluation forms - perform evaluations**: Allows a user, such as a Quality Assurance team member, to use an evaluation form to review a contact. For an example image, see Evaluate agent performance. Also allows them to search evaluations by evaluation form, score, last updated date/range, evaluator, and status.

- **Evaluation forms - manage form definitions**: Allows admins and managers to create and manage evaluation forms.

The **Admin** security profile has these permissions by default.

For information about how to add more permissions to an existing security profile, see Update security profiles.

Set up and review agent screen recordings

To help coach your agents to provide great customer service, you can use the Contact Lens screen recording feature to gain quality management insights. It records the agent's desktop, which helps you identify opportunities to improve performance. This information is also useful for ensuring compliance.

For example, let's assume it takes most agents two minutes to process a refund, but Jane Doe takes four minutes. You can watch a recording of her desktop when she's doing a refund and discover why she is taking longer.

The following diagram shows the architecture and workflow for screen recording. After the diagram there's a legend that explains each step.
1. Enable screen recording in the flow.
2. The agent accepts a contact that has screen recording enabled.
3. The agent's Contact Control Panel (CCP) connects with the Amazon Connect Client Service by using a web-socket (port 5431) to trigger screen recording.
4. The Amazon Connect Client Application uploads the screen recording video to the CCP.
5. The CCP uploads the screen recording to Amazon Connect in near-real time through HTTPS (port 443).
6. (Optional) You can use the `SuspendContactRecording` and `ResumeContactRecording` and APIs to pause and resume screen recording.
7. Amazon Connect initiates post processing of screen recording and merges the video with the call recording audio into an MP4 file.
8. Amazon Connect uploads the final MP4 file to your Amazon S3 bucket and encrypts the MP4 file using your KMS key.
9. Supervisors and quality assurance analysts view the screen recording on the **Contact details** page in Amazon Connect.
Important
Amazon Connect Contact Lens screen recording is not supported when you run the Contact Control Panel (CCP) across multiple applications at the same time.

Contents

- Amazon Connect Client Application
- Enable screen recording
- Troubleshoot: Download log files for the screen recording client app
- Assign security profile permissions for screen recordings
- Review agent screen recordings
- FAQ for screen recording capabilities

Amazon Connect Client Application

Download location

<table>
<thead>
<tr>
<th>Version</th>
<th>Release date</th>
<th>Download link</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0.2.38 (latest)</td>
<td>Sept 29, 2023</td>
<td><a href="#">AmazonConnectClientWin-v1.0.2.38</a></td>
</tr>
<tr>
<td>v1.0.1.33</td>
<td>July 21, 2023</td>
<td><a href="#">AmazonConnectClientWin-v1.0.1.33</a></td>
</tr>
<tr>
<td>v1.0.0.28</td>
<td>June 16, 2023</td>
<td><a href="#">AmazonConnectClientWin-v1.0.0.28</a></td>
</tr>
</tbody>
</table>

To be notified when there is an update to the Amazon Connect Client Application, we recommend subscribing to the RSS feed of this administrator guide. Choose the RSS link that appears under the title of this page (it's next to the PDF link).

**System requirements**

- CPU: 2.0GHz
- Memory: 2.5GB
- Network: 600Kbps
- Supported operating systems: 64-bit Windows 10 and 11 based on the x86-64 architecture

**Feature specifications**

- **Number of open applications that can be recorded**: All open applications on a monitor are recorded, up to 3 monitors.
- **Port used for screen recording**: The Amazon Connect Client Application communicates with the Contact Control Panel through a local websocket on port 5431.
- **IP addresses to add to your firewall allowlist**: To ensure smooth screen recording functionality, add to your allowlist the IP addresses associated with Amazon S3. These IP addresses are located in the `ipranges.json` file specific to your AWS Region. For example, if you are in us-east-1, add the S3 IP addresses for that Region to your allowlist.

**Enable screen recording**

**Step 1: Enable screen recording for your instance**

In this step you update your instance settings to enable screen recording.

- In the Amazon Connect console, choose your instance alias, choose Data storage, Screen recordings, Edit. You are prompted to create or choose an Amazon S3 bucket. After the bucket is created, you can store screen recordings and export them.

For instructions about navigating to your instance settings, see [Update instance settings](#).
Step 2: Download and install the Amazon Connect Client Application

In this step you install the Amazon.Connect.Client.Service file onto the agent's desktop, or into the virtual environment that the agent uses. This is the Amazon Connect Client Application. It records the agent's open applications.

1. **Download** the latest version of the Amazon.Connect.Client.Service.Setup file. This is an .MSI file.

2. Use your organization's software distribution mechanism, such as Software Center, to install the Amazon.Connect.Client.Service client app on agent desktops.

3. To verify the app is installed on the agent's desktop, navigate to C:\Program Files\Amazon\Amazon.Connect.Client.Service. Verify that the Amazon.Connect.Client.Service executable program is present.


(Optional) Step 3: Verify the Amazon Connect Client Application is running and functioning correctly

1. To verify that the application is running, check the Windows Task Manager for a background process named Amazon.Connect.Client.Service. This is the Amazon Connect Client Application.

2. To verify that the application is functioning correctly and creating log files, navigate to C:\ProgramData\Amazon\Amazon.Connect.Client.Service\logs.
   a. Open log files that are present in the directory.
   b. In a successful installation the log files contain the following line:

   "Checking that services are still running, result : true"

Step 4: Configure the Set recording and analytics behavior block

- Add a [Set recording and analytics behavior](#) block immediately after the point of entry to the flow. Add the block to every flow that you want to enable for screen recording.
The following image shows the properties page of the Set recording and analytics behavior block. In the Screen Recording section, choose On.

Configuration tips

- To enable supervisors to search for contacts that have screen recordings, add a Set contact attributes block before Set recording and analytics behavior. Add a custom attribute called something like screen recording = true. Supervisors can search on this custom attribute to find those that have screen recordings.

- You may want to add a Distribute by percentage block before Set recording and analytics behavior. This enables you to use screen recording for some but not all contacts.

- You may want to leverage the SuspendContactRecording and ResumeContactRecording APIs to prevent sensitive information from being captured in the screen recording.

Next steps

- Assign supervisors the required security profile permission: Analytics and optimization - Screen recording - Access.

- Show supervisors how to review screen recordings.
Troubleshoot: Download log files for the screen recording client app

When you open an AWS Support ticket for issues with screen recordings, provide the log files for the Amazon Connect Client Application on the agent's desktop and the browser shared worker.

How to access the Amazon Connect Client Application log files

- On the agent's desktop, navigate to C:\ProgramData\Amazon\Amazon.Connect.Client.Service\logs.

How to access the screen recording shared worker logs in the browser

⚠ Important
Before doing these steps, open your CCP. It must be open so you can view the ClientAppInterface shared worker.

- Chrome
  1. Open a Chrome browser. For the URL type chrome://inspect/#workers.
  2. In the Shared workers section, locate the shared worker named ClientAppInterface.
  3. Click inspect to open a DevTools instance.
  4. Choose the Console tab, right-click the log dump, and then select Save as... to store the log dump to a local file.

- Firefox
  1. Open a Firefox browser. For the URL type about:debugging#workers.
  2. In the Shared workers section, choose Inspect for /connect/ccp-naws/static/client-app-interface.js.
  3. Right-click the Console tab and select Save all Messages to File to store the log dump to a local file.

- Edge(Chromium)
  1. Open a Chrome browser. For the URL type edge://inspect/#workers.
  2. In the Shared workers section, locate the shared worker named ClientAppInterface.
  3. Choose inspect to open a DevTools instance.
4. Choose the **Console** tab, right-click the log dump, and then select **Save as...** to store the log dump to a local file.

### Assign security profile permissions for screen recordings

To allow users to review screen recordings, assign the following **Analytics and optimization** security profile permission:

- **Screen recording - Access**: Allows a user, such as a supervisor or Quality Assurance team member, to access and review screen recordings.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

### Review agent screen recordings

Use screen recordings to help you evaluate agents. You can identify areas for coaching, validate activity, or identify best practices.

The screen recording is synchronized with the voice recording and contact transcript, so you can hear or read what is being said at the same time.

1. Log in to Amazon Connect with a user account that has the **Analytics and optimization - Screen recording - Access** permission in its security profile.
2. On the navigation menu, choose **Analytics and optimization, Contact search**.
3. Search for the contact you want to review.

#### Tip

If you've added a custom attribute to your flows to indicate when screen recording is enabled, you can [search by the custom attribute](#) to locate contact records with screen recordings. For more information, see [Configuration tips](#).

4. Click or tap the contact ID to view the **Contact details** page.
5. The **Recording** section contains a video player that displays the screen recording, as shown in the following image.
6. Use the left-side controls to zoom in and out, or fit the video to the window.

7. Right-click while your cursor is on the video to display a full list of controls. They are shown in the following image.
8. If you don't see a video recording, check that the Show recording toggle is on.

If no video appears, then the screen recording may not yet be ready (that is, uploaded into the Amazon S3 bucket). If the problem persists, contact AWS Support Center.

**Watch in Picture-in-picture mode**

You may want to move the video elsewhere on your monitor while you watch it. For example, you can reposition the video so you can read the transcript. Use **Watch in Picture-in-picture** mode to achieve this.

1. Right-click the video to display the list of video controls.
2. Choose **Watch in Picture-in-picture**.

   The video windows pops out. You can move it around your monitor.
3. Choose the X in the top right corner to pop the window back. The following image shows the video in Picture-in-picture mode.
FAQ for screen recording capabilities

- **What operating systems are supported?**

  Windows 10 and 11 based on the x86 architecture.

- **What is the file format of screen recordings?**

  The screen recording files are saved in MP4 format.

- **Which Amazon Connect channels are supported?**

  You can generate screen recordings for voice, chat, and task contacts.

- **Where the logs located for the Amazon Connect Client Application?**

  You can locate the logs in `C:\Program Data\Amazon\Amazon.Connect.Client\Logs`.

- **Do you capture the entire screen?**

  Yes, the Amazon Connect Client Service records the all the open applications on the agent's monitor, up to three monitors.

- **Does screen recording support concurrent user sessions on Windows using Virtual Desktop Infrastructure (VDI) environments?**

  No, screen recording doesn’t support concurrent user sessions on Windows.
• Where are the screen recording files stored in my AWS account?

The screen recordings are delivered to your Amazon S3 bucket and encrypted using the KMS key you specify. This is similar to how call recordings are stored and encrypted.

• Where can I download the latest version of the Amazon Connect Client Application?

The download link is on the Amazon Connect Client Application page.

• How can I be notified when there is a latest version of the client application?

To be notified when there is an update to the Amazon Connect Client Application, we recommend subscribing to the RSS feed of this administrator guide. Choose the RSS link that appears under the title of this page (it's next to the PDF link).

• How are the recordings viewed?

Supervisors can view the screen recordings in the contact detail page, provided they have the necessary permissions enabled in their security profiles.

• What additional ports are used for screen recording?

The Amazon Connect Client Application communicates with the CCP through a local websocket on port 5431.

• What are the bandwidth requirements for screen recording?

We recommend 500kbps per concurrent contact with screen recording enabled.

• Can I opt only for screen recording and not for call recording?

Yes, you can enable screen recording without call recording for a voice call.

• How do I find the Amazon S3 location of the screen recording?

You can find the screen recording location in the RecordingsInfo section of the contact record. See the Location field.

• How do I enable screen recording for a percentage of my contacts?

You can use the Distribute by percentage block in the flow to enable a percentage of contacts for screen recording.

• Is screen recording PCI compliant?

Screen recording is Payment Card Industry Data Security Standard (PCI) compliant.

• Does screen recording work with custom CCP and agent desktops?
Screen recording is designed to work with custom CCP and agent workspace built with the Amazon Connect Streams JS library. We recommend testing your custom solution before deploying screen recording in production.

- What additional IP addresses do I need to add to my firewall allowlist?

To ensure smooth screen recording functionality, add to your allowlist the IP addresses associated with Amazon S3. These IP addresses are located in the ipranges.json file specific to your AWS Region. For example, if you are in us-east-1, add the S3 IP addresses for that Region to your allowlist.

- Can I use screen recording anywhere in the world?

Screen recording is available in all AWS commercial Regions where Amazon Connect is available. However, your use of screen recording may be subject to compliance with privacy and other laws. Please consult your compliance team before enabling this capability for your agents.

- Are agents alerted when screen recording is enabled for a contact?

By default Amazon Connect doesn't provide a notification feature. However, you can use the Amazon Connect Streams JS library to create a notice or other visual indicator on an agent's desktop to signal that screen recording is in use.

Search for contacts

**Note**

**New Feature:** You can now search for in-progress contacts on the Contact search page. This feature will be available by the end September, 2023, in all AWS Regions where Amazon Connect is supported.

Important things to know

- You can search for contacts as far back as two years ago.
- Amazon Connect returns search results for both completed and in-progress contacts. For contacts handled by agents, a contact is only marked as completed once the agent has completed After Contact Work (ACW).
For voice and chat contacts, the **Contact search** page displays in-progress contacts that are connected to an agent or disconnected. In-progress queued callbacks are not shown on the **Contact search** page.

For tasks, Contact search displays all in-progress contacts after they are initiated.

The search results for a given query are limited to the first 10K results returned.

When you filter by Contact ID, only results for that specific contact will be returned and other criteria are ignored. For example, say you search for Contact ID 12345 and agent login Jane Doe. Results for Contact ID 12345 will be returned regardless of whether Jane Doe was the agent.

You cannot search for multiple contact IDs at the same time.

### Key search features

- **Search by custom contact attributes** (user-defined attributes).
- **Search for contacts that are in progress** or completed using the **Contact status** filter.
- Search a time range up to 8 weeks. Within the time range filter, you can specify the **Timestamp type**. This enables you to specify the time range. You can choose from initiated, connected to agent, disconnected, and scheduled timestamps.

#### Important

- Time range filter on Contact search has Timestamp type set to "Initiated" by default. Before the Timestamp type selection was introduced, the Timestamp type used by the Time Range filter was "Disconnected".
- Saved searches on Contact search created prior to the launch of the ability to search for in-progress contacts (launched September 2023) have been updated with the filters Contact status = "Completed" and Timestamp type = "Disconnected". These selections were implied before the launch of in-progress contacts.

- Multi-select for filters such as agent names and contact queues.
- Filters for **Contact Lens for Amazon Connect**. You can **search for Contact categories** by specifying the full category name. Choose to search using **Match any** or **Match all** or **Match none**. For example, you can search contacts with both "category A" and "category B," or with either one of the two categories.
In the **Add filter** drop-down box, the Contact Lens filters have **CL** next to them. You can apply these filters only if your organization has enabled Contact Lens.

If you want to remove the Contact Lens filters from a user's drop-down list, remove the following permissions from their security profile:

- **Search contacts by conversation**: This controls access to the sentiment scores, non-talk time, and category searches.

- **Search contacts by keywords**: This controls access to the keywords search.

- **Contact Lens - conversational analytics**: On the **Contact details** page, this displays graphs that summarize conversational analytics.

- Filters for **Voice ID**. You can search for the Voice ID authentication and fraud detection status of contacts, if your organization has enabled Voice ID. To access this functionality, on your security profile, you need **Analytics and Optimization, Voice ID - attributes and search - View** permission.

The following image shows the filters available to search Voice ID: **Authentication result, Fraud detection result, Speaker actions**.

![Filters](image)
Manage who can search for contacts and access detailed information

Before users can search for contacts in Amazon Connect, or access detailed contact information, they need to be assigned to the CallCenterManager security profile, or have the following Analytics and Optimization permissions:

- **Access metrics - Access** (Required): Grants access to metrics data.
- At least one of the following permissions is required to view contacts on **Contact search** and **Contact details** pages:
• **Contact search - View**: Allows a user to access all contacts on **Contact search** and **Contact details** pages.

• **View my contacts - View**: On the **Contact search** and **Contact details** pages, allows agents to view only those contacts that they handled.

• **Restrict contact access** (Optional): Manage a user’s access to results on the **Contact search** page based on their agent hierarchy group.

For example, agents who are assigned to AgentGroup-1 can only view contact records for contacts handled by agents in that hierarchy group, and any groups below them. (If they have permissions for **Recorded conversations**, they can also listen to call recordings and view transcripts.) Agents assigned to AgentGroup-2 can only access contact records for contacts handled by their group, and any groups below them.

Managers and others who are in higher level groups can view contact records for contacts handled by all the groups below them, such as AgentGroup-1 and 2.

For this permission, **All = View** since **View** is the only action granted.

For more information about hierarchy groups, see [Set up agent hierarchies](#).

---

⚠️ **Important**

- Deleting a hierarchy level severs the link to existing contacts. This action cannot be reversed.

- When you change a user’s hierarchy group, it may take a couple of minutes for their contact search results to reflect their new permissions.

---

The following table lists the typical permissions and what contacts can be viewed on **Contact search** and **Contact details** pages.
<table>
<thead>
<tr>
<th>Contact search permission</th>
<th>View My Contacts permission</th>
<th>Restrict Contact Access permission</th>
<th>Which contacts can be viewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>All</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All contacts within your agent hierarchy, handled by an agent at your hierarchy level or below.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Only contacts handled by the user (agent) to whom the permission is granted.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No contacts</td>
</tr>
</tbody>
</table>

⚠️ **Important**

We do not recommend assigning permissions in any other combination than what is shown in the preceding table.

- **Contact Lens - conversational analytics**: On the **Contact details** page for a contact, you can view graphs that summarize conversational analytics: customer sentiment trend, sentiment, and non-talk time.

- **Recorded conversations (redacted)**: If your organization uses Contact Lens for Amazon Connect, you can assign this permission so agents access only those call recordings and transcripts in which sensitive data has been removed.

- **Recorded conversations (unredacted)**: If your organization isn't using Contact Lens, agents need **Recorded conversations (unredacted)** to listen to call recordings or view transcripts. If desired, you can use **Restrict contact access** to ensure they only have access to detailed information for those contacts handled by their hierarchy group.

- **Evaluation forms - perform evaluations**: Allows users to **search for** evaluations by evaluation form, score, last updated date/range, evaluator, and status.
• **Voice ID - attributes and search**: If your organization uses Voice ID, users with this permission can search for and view Voice ID results in the **Contact detail** page.

• **Users - View** permission: You must have this permission to use the **Agent** filter on the **Contact search** page.

By default, the Amazon Connect **Admin** and **CallCenterManager** security profiles have these permissions.

For information about how to add more permissions to an existing security profile, see **Update security profiles**.

### How to search for a contact

1. Log in to Amazon Connect with a user account that has permissions to access contact records.
2. In Amazon Connect choose **Analytics and optimization, Contact search**.
3. Use the filters on the page to narrow your search. For date, you can search up to 8 weeks at a time.

**Tip**

To see if a conversation was recorded, you need to be assigned to a profile that has **Manager monitor** permissions. If a conversation was recorded, by default the search result will indicate so with an icon in the **Recording** column. You won't see this icon if you don't have permission to review the recordings.

### Additional fields: Add columns to your search results

Use the options under **Additional fields** to add columns in your search results. These options are not used to filter your search.

For example, if you want to include columns for **Agent Name** and **Routing profile** in your search output, choose those columns here.
Tip

The **Is transferred out** option indicates whether the contact was transferred to an external number. For the date and time (in UTC time) when the transfer was connected, see `TransferCompletedTimestamp` in the `ContactTraceRecord`.

Download search results

You can download up to 3,000 search results at a time.

Search for in-progress contacts

Note

**New Feature:** You can now search for in-progress contacts on the **Contact search** page. This feature will be available by the end September, 2023, in all AWS Regions where Amazon Connect is supported.

For a contact that is handled by an agent, a contact is considered **In Progress** until the agent completes After Contact Work. For a contact that is never handled by an agent, a contact is considered **In Progress** until the contact is disconnected.

Permissions needed to search for in-progress contacts

The permissions needed to search for in-progress contacts are the same as those for searching for completed contacts. For more information, see Manage who can search for contacts and access detailed information.

Contact states supported by Contact search

For voice and chat contacts, the **Contact search** page displays in-progress contacts that are connected to an agent or disconnected. In-progress queued callbacks are not displayed on the **Contact search** page.

For tasks, the **Contact search** displays all in-progress contacts after they are initiated.
How to search for in-progress contacts

1. Log in to Amazon Connect with a user account that has permissions to access contact records.
2. In Amazon Connect choose Analytics and optimization, Contact search.
3. Select the Contact status filter and change the selected value to In progress. The default Contact status is Completed.

Filter contacts by using timestamp types

You can search for contacts in a particular contact state using Timestamp type within the Time range filter. For example, you can search for task contacts that are scheduled for the next day by selecting Contact status = In progress, Timestamp type = Scheduled and the appropriate date within Time range.

The following timestamp types are supported: initiated, connected (to agent), disconnected and scheduled. When you search for contacts using a certain Timestamp type, the search results do not contain contacts that do not have that timestamp populated, e.g. if you search for a contact with Timestamp type = Disconnected and Contact status = In progress, then you will only view contacts that are in After Contact Work state.

⚠️ Important

- The Time range filter on the Contact search page has Timestamp type set to Initiated by default. Before the Timestamp type selection was introduced, the Timestamp type used by the Time range filter wasDisconnected.
• Saved searches on **Contact search** created before to the launch of the ability to search for in-progress contacts (launched September 2023) have been updated with the filters **Contact status = Completed** and **Timestamp type = Disconnected**. These selections were implied before the launch of in-progress contacts.

**View in progress contacts**

You can click on a Contact ID within the **Contact search** results to view details of an in-progress contact.

![Contact details](image)

**Important things to know**

• The **Contact details** page for an in-progress contact shows data available at the time **Contact details** page was opened. It does not automatically refresh as the contact progresses. You need to refresh the page manually using your browser.

• Certain fields on **Contact search** and **Contact details** page may have missing or inconsistent information while the contact is in progress. After a contact is completed, information is eventually made consistent with the underlying contact record, after the page is manually refreshed.

• There may be a delay between the contact being **Completed** and the contact being marked as **Completed** on the contact record.

**Review real-time transcripts**

For voice contacts, with real-time call analytics enabled, you can view transcripts of a contact in real-time on a **Contact Details** page. Scrolling down within the transcript automatically pulls the
latest available turn of the conversation. Alternatively, you can choose the refresh icon on the bottom the transcript to see the latest conversation.

Search by custom contact attributes

You can create search filters based on custom contact attributes (also called user-defined contact attributes). For example, if you add AgentLocation and InsurancePlanType to your contact records as custom attributes, you can search for contacts with specific values in these attributes, such as calls handled by agents located in Seattle, or calls made by customers who purchased homeowners insurance.

Required permissions to configure searchable contact attributes

By default, a custom attribute isn't indexed until someone with appropriate permissions, such as an admin or manager, specifies it should be searchable. You grant permissions to select users so they can configure which custom contact attributes can be added as a search filter.
Assign the following permissions to their security profile:

- Enable one of the following permissions to access the **Contact Search** page:
  - **Contact search**: Allows you to search for all contacts.
  - **View my contacts**: Allows agents to view only those contacts that they handled.
  - **Contact attributes**: Allows users to view contact attributes. Also controls access to the search filters based on contact attributes.
  - **Configure searchable contact attributes - All**: People who have this permission determine what custom data will be searchable (by people who have the **Contact attributes** permission). It allows them to access the following configuration page:

![Configure searchable custom contact attributes](image)

**Configure searchable custom contact attributes**

1. On the **Contact search** page, choose **Add filter, Custom contact attribute**. Only people with **Configure searchable contact attributes** permissions in their security profile see this option.
2. The first time you choose **Custom contact attribute**, the following box appears, indicating no attributes have been configured for this Amazon Connect instance. Choose **Specify searchable attribute keys.**

3. In the **Attribute key** box, type the name of your custom attribute, and then choose **Add key.**

   **Important**

   You must type the exact key name. It is case sensitive.

4. When finished, choose **Save.**

   Your users will be able to search on these keys for any future contacts.
Edit, add, or remove contact attributes

To edit, add, or remove keys, choose **Attribute**, **Settings**. If you don't see the **Settings** option, you don't have the required permissions.

![Attribute Settings](image)

Search for custom contact attributes

Users who have the **Contact attributes** permission in their security profile can find contacts by using the contact attribute filters.

1. On the **Contact search** page, choose **Add filter**, **Custom contact attribute**, and then choose **Specify searchable attribute keys**.
2. On the **Searchable customer contact attributes** page, in the **Attribute key** box, enter the attribute key, and choose **+Add key** and then choose **Save**.
3. Return to the **Contact search** page. Use **Add filter** to choose from the dropdown menu the attribute you just added. In the **Attribute value box**, enter the value you want to find.

Monitor live and recorded conversations

The topics in this section explain how to monitor (listen-in) on conversations between agents and contacts.

Contents

- Set up live monitoring for voice and/or chat
- Assign permissions to monitor live conversations
- Listen to live conversations or read live chats
• **Barge live conversations**

• **Review recorded conversations between agents and customers using Amazon Connect**

• **Troubleshoot monitoring agent conversations with Amazon Connect**

## Set up live monitoring for voice and/or chat

Managers and agents in training can monitor live conversations between agents and customers. To set this up, you need to add the **Set recording behavior** block to your voice/chat flow, assign managers and trainees the appropriate permissions, and then show them how to monitor the conversations.

**Looking for how many people can monitor the same conversation at one time?** See Amazon Connect feature specifications.

There is no limit to the number of conversations that can be monitored in an instance.

### Add a Set recording and analytics behavior block to your flow

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>
| • **For monitoring voice calls**: This step is only required if you have not selected *Enable Multi-Party Calls and Enhanced Monitoring* in the Amazon Connect console. If you do have it enabled for your instance, then you no longer need to add the **Set recording and analytics behavior** block to your voice flow to set up monitoring. However, you still need to **assign permissions** to managers and trainees, and then show them **how to monitor conversations**.

• **For monitoring chats**: The **Set recording and analytics behavior** block is required to activate monitoring, regardless of the setting for *Enable Multi-Party Calls and Enhanced Monitoring*.

1. Add the **Set recording and analytics behavior** block to your flow. Do this to monitor calls, chats, or both.

   To enable monitoring of voice and/or chat conversations, on the block's **Properties** page choose **Agent and Customer**.
For more information, see Set up recording behavior.

2. Choose whether to record the conversations you monitor.

Although you need to add the Set recording behavior block to your flow, you don't need to record voice and/or chat conversations for monitoring to work. By default when you set up your instance, Amazon S3 buckets are created to store call recordings and chat transcripts. The existence of these buckets enables call recording and chat transcripts at the instance level.

To not record the calls or chats you're monitoring, disable the Amazon S3 buckets. For instructions, see Update instance settings.

Now you're ready to assign the necessary permissions to managers so they can monitor conversations. Continue to Assign permissions to monitor live conversations.

**Assign permissions to monitor live conversations**

For managers to monitor live conversations, you assign them the CallCenterManager and Agent security profiles. To allow agent trainees to monitor live conversations, you may want to create a security profile specific for this purpose.

**To assign a manager permissions to monitor a live conversation**

1. Go to Users, User management, choose the manager, and then choose Edit.
2. In the Security Profiles box, assign the manager to the **CallCenterManager** security profile. This security profile also includes a setting that makes the icon to download recordings appear in the results of the **Contact search** page.

3. Assign the manager to the **Agent** security profile so they can access the Contact Control Panel (CCP), and use it to monitor the conversation.

4. Choose **Save**.

**To create a new security profile for monitoring live conversations**

1. Choose **Users, Security profiles**.
2. Choose **Add new security profile**.
3. Expand **Analytics and optimization**, then choose **Access metrics** and **Real-time contact monitoring**.

   **Access metrics** is needed so they can access the real-time metrics report, which is where they choose which conversations to monitor.

4. Expand **Contact Control Panel**, then choose **Access Contact Control Panel** and **Make outbound calls**.

   ![Contact Control Panel (CCP)](image)

   These permissions are needed so they can monitor the conversation through the Contact Control Panel.

5. Choose **Save**.

Next, show your managers how to monitor conversations. Continue to [Listen to live conversations or read live chats](#).

**Listen to live conversations or read live chats**

Before you can listen to live conversations or read live chats, the Amazon Connect admin needs to [set up](#) the feature, and [assign you permissions](#). After that's done, you can do these steps.
For information about how many people can listen in to a conversation or follow a chat, see Amazon Connect feature specifications.

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that has the **Real-time contact monitoring** security profile permission.

2. Open the Contact Control Panel (CCP) by choosing the phone icon in the top-right corner of your screen. You'll need the CCP open to connect to the conversation.

3. To choose the agent conversation you want to monitor, in Amazon Connect choose **Analytics and optimization, Real-time metrics, Agents**. The following image shows the **Real-time metrics** page, with an arrow pointing to the **Agents** option.

4. To monitor voice conversations: Next to the names of agents in a live voice conversation, there is an eye icon. Choose the icon to start monitoring the conversation. The following image shows the eye icon next to the **Voice** channel.
When you're monitoring a conversation, the status in your CCP changes to **Monitoring**.

5. To monitor chat conversations: For each agent you'll see the number of live chat conversations they're in. Click on the number. Then choose the conversation you want to start monitoring.

   When you're monitoring a conversation, the status in your CCP changes to **Monitoring**.

6. To stop monitoring the conversation, in the CCP choose **End call** or **End chat**.

   When the agent ends the conversation, monitoring stops automatically.

**Barge live conversations**

Supervisors and managers can barge into live conversations between agents and customers. To set this up, you need to turn on the **Enhanced monitoring** capability in the Amazon Connect console, provide managers with the appropriate permissions, and show them how to barge into conversations.

**Looking for how many people can barge the same conversation at one time?** See [Amazon Connect feature specifications](https://aws.amazon.com/connect/feature-specifications/).

There is no limit to the number of conversations that you can barge in an instance.

The barge feature is included in Amazon Connect voice service fees. For pricing, see the [Amazon Connect Pricing](https://aws.amazon.com/connect/pricing/) page.
Set up barge for voice

in Amazon Connect console, select **Enable Multi-Party Calls and Enhanced Monitoring**. This option enables access to multi-party calling, detailed contact records, silent monitoring, and barge capabilities.

The following image shows the **Enable Multi-Party Calls and Enhanced Monitoring** option on the **Telephony Options** page.

![Telephony Options](image)

**Note**

- If multi-party calling is already enabled, to also you enable enhanced monitoring you will need to use the **UpdateInstanceAttribute** API with the **ENHANCED_CONTACT_MONITORING** attribute for the first time. Or, you can turn the feature OFF and then back ON to update your settings. For more information, see **UpdateInstanceAttribute** in the Amazon Connect API Reference Guide.

- Any new instances will automatically have this feature enabled.

- Before enabling **Enhanced monitoring** capabilities, ensure that you are using the latest version of the Contact Control Panel (CCP) or Agent workspace. If you are using StreamsJS to customize or embed the CCP, upgrade to version 2.4.2 or later.

- For instances that do not have a service-linked role, you must create one in order to enable the feature. For more information on how to enable service-linked roles, see **Use service-linked roles for Amazon Connect**.
Set up barge for voice

For managers to barge live conversations, you assign them the CallCenterManager and Agent security profiles. To allow specific users to barge live conversations, we recommend that you create a security profile specific for this purpose.

For the number of supervisors who can monitor a call at the same time, see Amazon Connect feature specifications.

To assign a manager permissions to barge a live conversation

1. Log in to the Amazon Connect admin website at https://instance name.my.connect.aws/. Use an Admin account, or an account assigned to a security profile that has permissions to assign security profile permissions.
2. On the navigation menu, choose Users, User management. Choose the manager, and then choose Edit.
3. In the Security Profiles box, assign the manager to the CallCenterManager security profile.
4. Assign the manager to the Agent security profile so they can access the Contact Control Panel (CCP), and use it to barge into the conversation.
5. Choose Save.

To create a new security profile for monitoring live conversations

2. Choose Add new security profile.
3. Expand Analytics and choose Real-time contact barge-in, as shown in the following image.
For a manager to use the barge feature, both **Real-time contact monitoring** and **Real-time contact barge** need to enabled.

*Access metrics* is needed so you can access real-time metrics reports, which is where you choose which conversation you would like to monitor.

4. Choose **Save**.

### Barge live calls with contacts

1. Log in to the Amazon Connect admin website at https://*instance name*.my.connect.aws/..
   Use an account that is assigned the **CallCenterManager** security profile or a user that has been given **Real time contact monitor** and **barge** permissions.

2. On the navigation menu, choose **Analytics and optimization, Real-time metrics, Agents**.

3. Choose the eye icon that appears next to the **Voice** channel of the agent that you want to monitor, as shown in the following image. You can barge into a conversation that you had been monitoring already.
4. This opens the Contact Control Panel (CCP), as shown in the following image. You can enable barge, and move between the **Monitor** and **Barge** states.

**Review recorded conversations between agents and customers using Amazon Connect**

Managers can review past conversations between agents and customers. To set this up, you need to [set up recording behavior](#), assign managers the appropriate permissions, and then show them how to access the recorded conversations.

**When is a conversation recorded?** A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the IVR or a Lex bot. If the call is transferred externally, the call recording stops when the agent drops from the call. For detailed information about call recording behavior, see [Set up recording behavior](#)
Tip
When call recording is enabled, the recording is placed in your S3 bucket shortly after the contact is disconnected. Then the recording is available for you to review it using the steps in this article.
You can also access the recording from the customer's contact record. The recording is available in the contact record, however, only after the contact has left the After Contact Work (ACW) state.

How do I manage access to recordings? Use the Recorded conversations (unredacted) security profile permission to manage who can listen to recordings, and access the corresponding URLs that are generated in S3. For more information about this permission, see Assign permissions to review recordings of past conversations.

Assign permissions to review recordings of past conversations

Assign the CallCenterManager security profile so a user can listen to call recordings or review chat transcripts. This security profile also includes a setting that makes the icon to download recordings appear in the results of the Contact search page. The following image shows the recording play, download, and delete icons that are displayed to a user who has these permissions.

Or, assign the following individual permissions.

1. **Contact search**: This permission is required so users can access the Contact search page, which is where they can search contacts so they can listen to recordings and review transcripts.
2. **Restrict contact access**: Manage access to results on the Contact search page based on their agent hierarchy group.

   For example, agents who are assigned to AgentGroup-1 can only view contact trace records (CTRs) for contacts handled by agents in that hierarchy group, and any groups below them. (If they have permissions for Recorded conversations, they can also listen to call recordings and view transcripts.) Agents assigned to AgentGroup-2 can only access CTRs for contacts handled by their group, and any groups below them.
Managers and others who are in higher level groups can view CTRs for contacts handled by all the groups below them, such as AgentGroup-1 and 2.

For this permission, All = View since View is the only action granted.

For more information about hierarchy groups, see Set up agent hierarchies.

>Note

When you change a the hierarchy group of a user, it may take a couple of minutes for their contact search results to reflect their new permissions.

3. **Recorded conversations (redacted):** If your organization uses Contact Lens for Amazon Connect, you can assign this permission so agents access only those call recordings and transcripts in which sensitive data has been removed.

   The redaction feature is provided as part of Contact Lens for Amazon Connect. For more information, see Use sensitive data redaction.

4. **Manager monitor:** This permission allows users to monitor live conversations and listen to recordings.

>Tip

Be sure to assign managers to the Agent security profile so they can access the Contact Control Panel (CCP). This enables them can monitor the conversation through the CCP.

5. **Recorded conversations (unredacted):** If your organization isn’t using Contact Lens for Amazon Connect, use this permission to manage who can access recordings on the Details page, through corresponding URLs that are generated in S3. From there, these users can delete recordings.

   Note the following:

   - To restrict access to recordings, ensure users do not have Analytics and Optimization - Recorded conversations (unredacted) - Access permissions, as shown in the following image.
If users do not have **Recorded conversations** permission—or they're not logged in to Amazon Connect—they cannot listen to the call recording or view the chat transcript, or access the URL in S3, even if they know how the URL is formed.

The **Enable download button** permission controls only whether the download button appears in the user interface. It does not control access to the recording.

To enable a user to delete recordings, choose the **Delete** permission. To view the **Delete** button in the Amazon Connect admin website, you need the **Enable download button** permission. The **Enable download button** permissions are granted by default when you assign the **Delete** permission.

### Review recordings/transcripts of past conversations

These are the steps that a manager does to review past recordings/transcripts of conversations.

1. Log in to Amazon Connect with a user account that has permissions to access recordings.
2. In Amazon Connect choose **Analytics and optimization, Contact search**.
3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose **Search**.

#### Tip

We recommend using the **Contact ID** filter to search for recordings. This is the best way to ensure you get the right recording for the contact. Many recordings have the same name as the contact ID, but not all.

4. Conversations that were recorded have icons in the **Recording/Transcript** column, as shown in the following image. If you don't have the appropriate permissions, you won't see these icons.
5. To listen to a recording of a voice conversation, or read the transcript of a chat, choose the **Play** icon, as shown in the following image.

6. If you choose the play icon for a transcript, it appears, as shown in the following image.

### Pause, rewind, or fast-forward a recording

Use the following steps to pause, rewinder, or fast-forward a voice recording.

1. On the **Contact search** results, instead of choosing the **Play** icon, choose the contact ID to open the contact record.
2. On the **Contact record** page, there are more controls to navigate the recording, as shown in the following image.

1. Click or tap to the time you want to investigate.
2. Adjust the playing speed.
3. Play, pause, skip backwards or forwards in 10 second increments.
Troubleshoot problems pausing, rewinding, or fast-forwarding

If you are unable to pause, rewind or fast-forward recordings on the Contact search page, one possible reason could be that your network is blocking HTTP range requests. See HTTP range requests on the MDN Web Docs site. Work with your network administrator to unblock HTTP range requests.

Download recordings/transcripts of past conversations

These are the steps that a manager does to download past recordings or transcripts of conversations.

- If the contact reached you by phone call (the Voice channel), you can download a .wav file.
- If the contact reached you by chat (the Chat channel), you can download a .json file.

Tip

To have Amazon Connect create transcripts of phone calls, see the Contact Lens feature. However, you can't download the recording or transcript.

To download a voice recording as a .wav file

1. Log in to Amazon Connect with a user account that has permissions to access recordings.
2. In Amazon Connect choose Analytics and optimization, Contact search.
3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose Search.
4. Conversations that were recorded have icons in the Recording/Transcript column. If you don't have the appropriate permissions, you won't see these icons.

The following image shows what the icons look like for a voice recording. Note the play icon that indicates it's a voice recording.

5. Choose the Download icon, as shown in the following image.
6. A voice recording is saved automatically to your Downloads folder as a .wav file.

The following image shows a list of .wav files in a Downloads folder. The name of the .wav file is the contact ID.

![Image of .wav files]

Tip

In the recording, you may hear only the agent, only the customer, or both the agent and customer. This is determined by how the Set recording and analytics behavior block is configured.

To download a chat transcript as a .json file

1. The following image shows what the icons look like for a chat transcript.

![Image of chat transcript]

A chat transcript is saved to the Downloads folder as a .json file.

The following image shows a .json file in the Downloads folder. The name of the .json file is the contact ID.

![Image of .json file]

Review recorded conversations
2. To view a downloaded chat transcript, right-click the .json file, and then open it with another app that enables you to view the contents in a readable format.

The following image shows a sample downloaded transcript that has been opened using Firefox. The image shows the middle of the transcript, where the agent and customer are chatting.

Search for recordings by contact ID

To find a recording of a specific contact, you only need the contact ID. You don't need to know the date range, agent, or any other information about the contact.

Tip

We recommend using the contact ID to search for recordings. Even though many call recordings for specific contact IDs may be named with the contact ID prefix itself (for example, 123456-aaaa-bbbb-3223-2323234.wav), there is no guarantee that the contact IDs and name of the contact recording file always match. By using Contact ID for your search on the Contact search page, you can find the correct recording by referring the audio file on the contact's record.

To search for recordings

1. Log in to Amazon Connect with a user account that has permissions to access recordings.
2. In Amazon Connect choose **Analytics and optimization, Contact search**.

3. In the **Contact ID** box, enter the contact ID, and then choose **Search**.

4. Conversations that were recorded have icons in the **Recording/Transcript** column. The following image shows the play, download, and delete icons. If you don't have the appropriate permissions, you won't see these icons.

To learn more about searching, see [Search for contacts](#).

### Troubleshoot monitoring agent conversations with Amazon Connect

The following table explains how to resolve error messages (exception messages) that may be displayed when you use Amazon Connect to monitor live agent conversations with contacts.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
<th>Exception type</th>
<th>Exception code</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>One or more of the input parameters are invalid</strong></td>
<td>A developer needs to make sure that the input parameters for the <strong>MonitorContact</strong> action are valid. See <a href="#">MonitorContact Request Syntax</a>.</td>
<td><strong>InvalidRequestException</strong></td>
<td><strong>400</strong></td>
</tr>
<tr>
<td><strong>Monitoring failed, please enable call recording</strong></td>
<td>In the flow, make sure that the <strong>Set recording and analytics behavior</strong> block is configured to allow call recording for both the agent and customer.</td>
<td><strong>InvalidRequestException</strong></td>
<td><strong>400</strong></td>
</tr>
<tr>
<td>Error message</td>
<td>Resolution</td>
<td>Exception type</td>
<td>Exception code</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>User's phone number is invalid</td>
<td>Check that the phone number associated with the agent's deskphone meets following requirements:</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td></td>
<td>1. It is a valid phone number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. It is in the required E164 format. To express a US phone number in E.164 format, add the '+ prefix and the country code in front of the number. For example, for a US number +1-800-555-1212. A number such as 020 718 xxxx in the UK would be formatted as +44 20 718 xxxx.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. It is in the list of countries that Amazon Connect can call. For a list of countries allowed by default, see Countries you can call by default.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For example, your Amazon Connect instance is in the US East (N. Virginia) Region. Your agent has a deskphone in Germany, which is not a country that Amazon Connect can call by default. By default the agent's deskphone would not be configured correctly to start the monitoring session so they would get an error. You would need to submit a service quota increase request to add Germany to your list of allowed countries that Amazon Connect can call.

4. The queue that is associated with the agent's routing profile has an outbound caller ID number assigned
<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
<th>Exception type</th>
<th>Exception code</th>
</tr>
</thead>
<tbody>
<tr>
<td>The contact or agent is not in the state that can be monitored</td>
<td>The contact is not in an active state. The agent or customer may have disconnected from the call or chat before the monitoring request could be processed. Choose another contact to monitor.</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td>Monitoring failed, please enable multi party conferencing feature</td>
<td>The Amazon Connect instance must have the multi-party calls and enhanced monitoring feature enabled. In your instance settings, choose Enable Multi-Party Calls and Enhanced Monitoring. For instructions, see Update instance settings.</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td>Error message</td>
<td>Resolution</td>
<td>Exception type</td>
<td>Exception code</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>No AGENT participant found in the contact</td>
<td>The call or chat doesn't have an active agent who is connected to it and working on the contact. Choose another contact to monitor.</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td>MonitorContact is not supported for TASK contacts</td>
<td>The monitoring feature is supported only for voice and chat contacts. Choose a voice or chat contact to monitor.</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td>AllowedMonitorCapabilities must be provided and have SILENT_MONITOR value at the least</td>
<td>If your Amazon Connect instance has the multi-party calls and enhanced monitoring feature enabled, the developer must make sure to pass the AllowedMonitorCapabilities input parameter with at least the SILENT_MONITOR value set. See MonitorContact Request Syntax.</td>
<td>InvalidRequestException</td>
<td>400</td>
</tr>
<tr>
<td>Error message</td>
<td>Resolution</td>
<td>Exception type</td>
<td>Exception code</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>One or more of the request resources were not found</td>
<td>A developer needs to make sure that the resources in the MonitorContact input request that's being passed exist in the Amazon Connect instance.</td>
<td>ResourceNotFoundException</td>
<td>404</td>
</tr>
<tr>
<td>Internal service exception</td>
<td>The request processing has failed because of an unknown error, exception, or failure with an internal server. Wait a bit and then try again to monitor the contact.</td>
<td>InternalServiceException</td>
<td>500</td>
</tr>
<tr>
<td>Service quota has been exceeded</td>
<td>There are certain limits on how many contacts a supervisor can monitor at a time or how many supervisors can monitor one contact. Check the limits for the voice and chat contacts on the Amazon Connect feature specifications page.</td>
<td>ServiceQuotaException</td>
<td>402</td>
</tr>
<tr>
<td>Error message</td>
<td>Resolution</td>
<td>Exception type</td>
<td>Exception code</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Another request with same clientToken is in progress</td>
<td>In the MonitorContact action, a ClientToken is a unique, case-sensitive identifier that developers provide to ensure the idempotency of the request. If not provided, the AWS SDK populates this field. For more information about idempotency, see Making retries safe with idempotent APIs.</td>
<td>IdempotencyException</td>
<td>409</td>
</tr>
<tr>
<td>Access denied</td>
<td>You don't have the appropriate permissions in your security profile to perform this action. For a list of the security profile permissions required for monitoring conversations see Assign permissions to monitor live conversations.</td>
<td>AccessDeniedException</td>
<td>403</td>
</tr>
</tbody>
</table>
Manage contacts from the Contact details page

On the Contact details page of an in-progress contact, you can manage a contact by transferring, rescheduling, or ending the contact.

You can also perform these actions programmatically using the TransferContact, UpdateContactSchedule, and StopContact operations.

This section explains how to transfer, reschedule, and end contacts by using the Amazon Connect admin website.

Contents

- Transfer contacts from the Contact details page
- Reschedule contacts from the Contact details page
- End contacts from the Contact details page

Transfer contacts from the Contact details page

On the Contact details page of an in-progress contact, you can transfer a contact to a quick connect agent or queue. This capability is currently supported only for task contacts.

To transfer contacts programmatically, use the TransferContact.

Required permissions

1. Enable one of the following permissions to view contacts on the Contact search and Contact details pages:
a. **Contact search - View**: Allows a user to view all contacts

b. **View my contacts - View**: Allows agents to view contacts that they themselves had handled

2. **Restrict contact access** (Optional): Restrict a user's access to contacts on the **Contact search** and **Contact details** pages within their own hierarchy group or any hierarchy groups below them. For more information about this permissions, see Manage who can search for contacts and access detailed information.

3. **Transfer Contact**: Enables a user to transfer contacts on the **Analytics & Optimization** pages. The following image shows the **Contact Actions - Transfer Contact** permission.

![Contact Actions](image)

**How to transfer a contact**

1. Log in to Amazon Connect with a user account that has permissions to access contact records.
2. In Amazon Connect choose **Analytics and optimization, Contact search**.
3. Search for an in-progress task contact to transfer:
   a. Select the **Contact status** filter and set it to **In progress**, as shown in the following image.
b. Set the Channel filter to Tasks to view only task contacts.

c. Choose the task contact to view its details.

4. On the Contact details page for the task contact, choose Actions, Transfer.

5. Select an agent or queue from a list of your quick connects and choose Transfer.

6. When the contact is transferred successfully, the page automatically refreshes with the Next contact link to the contact created as a result of the transfer. The following image shows the location of the Next contact link.
Reschedule contacts from the Contact details page

On the Contact details page of an in-progress contact, you can reschedule a contact that was previously scheduled. This capability is currently supported only for task contacts.

To reschedule contacts programmatically, use the UpdateContactSchedule.

Required permissions

1. Enable one of the following permissions to view contacts on the Contact search and Contact details pages:
   a. Contact search - View: Allows a user to view all contacts
   b. View my contacts - View: Allows agents to view contacts that they themselves had handled

2. Restrict contact access (Optional): Restrict a user’s access to contacts on the Contact search and Contact details pages within their own hierarchy group or any hierarchy groups below them. For more information about this permissions, see Manage who can search for contacts and access detailed information.

3. Reschedule contact: Enables a user to reschedule contacts on the Analytics & Optimization pages. The following image shows the Contact Actions - Reschedule contact permission.
How to reschedule a contact

1. Log in to Amazon Connect with a user account that has permissions to access contact records.
2. In Amazon Connect choose Analytics and optimization, Contact search.
3. Search for an in-progress task contact to reschedule:
   a. Select the Contact status filter and change the selected value to In progress.
   b. Select the Time range filter. Set the Timestamp type to Scheduled to view only scheduled contacts. Filter for the time range. The following image shows these filters.
4. Choose the scheduled contact to view its details.
5. On the Contact details page of the task contact, choose Actions, Reschedule, as shown in the following image.
6. Select the time and range to reschedule the contact. The scheduled time must be within 6 days of when the task was initiated.

7. When the contact is rescheduled successfully, the page automatically refreshes with the new schedule time for the task.

End contacts from the Contact details page

On the Contact details page of an in-progress contact, you can end a contact. Ending a contact results in the contact being disconnected. If the contact was already connected to an agent, ending the contact starts After Contact Work (ACW) for the contact.

To end contacts programmatically, use the StopContact.

Important things to know

- If you end a task contact after ACW is in progress, the contact is terminated. Voice and chat contacts that are in ACW state cannot be terminated by performing End contact action on the Contact details page.
- You cannot end voice contacts when they are initiated using the following methods:
  - DISCONNECT
  - TRANSFER
  - QUEUE_TRANSFER
- You can end chat and task contacts regardless of how they were initiated.

Required permissions

1. Enable one of the following permissions to view contacts on the Contact search and Contact details pages:
a. **Contact search - View**: Allows a user to view all contacts.

b. **View my contacts - View**: Allows agents to view contacts that they themselves had handled.

2. **Restrict contact access** (Optional): Restrict a user's access to contacts on the **Contact search** and **Contact details** pages within their own hierarchy group or any hierarchy groups below them. For more information about this permissions, see [Manage who can search for contacts and access detailed information](#).

3. **End Contact**: Enables a user to end contacts on the **Analytics & Optimization** pages. The following image shows the **Contact Actions - End contact** permission.

![Contact Actions](image)

**How to end an in-progress contact**

1. Log in to Amazon Connect with a user account that has [permissions to access contact records](#).

2. In Amazon Connect choose **Analytics and optimization**, **Contact search**.

3. Select the **Contact status** filter and change the selected value to **In progress**.

4. Choose an in-progress contact to view its details.

5. On the **Contact details** page choose **Actions**, **End**.

6. Confirm the action to end the contact by choosing **End**.

7. When the contact is ended successfully, the page automatically refreshes.
Use Customer Profiles

To help agents deliver more efficient and personalized customer service, Amazon Connect enables you to combine information from external applications, such as Salesforce, Zendesk, ServiceNow, or other Customer relationship management (CRM) products, with contact history from Amazon Connect. This creates a customer profile that has all the information agents need during customer interactions in a single place.

With a single view of customer information including their product, case, and contact history, agents can quickly confirm the customer's identity and determine the reason for the call or chat.

Currently, Amazon Connect Customer Profiles can be used in compliance with GDPR and is pending additional certifications held by Amazon Connect.

The following image shows the agent workspace; for the purposes of this documentation, an Amazon Connect Customer Profiles image is featured. The agent workspace is designed for efficient multi-tasking, enabling simultaneous handling of calls, chats, and tasks, while providing quick access to customer profile information all within the same browser window.

1. **Cases**: Status, reference Id, title, source, updated date, and more information related to cases ingested from 3P application such as Zendesk and ServiceNow, in addition to cases created and managed using Amazon Connect Cases.
2. **More information**: Additional information contained in the customer defined *Attributes* field of the profile, as well as further profile information such as cell phone number and shipping address. This information will be sorted alphabetically to help an agent quickly locate the information they need.

3. **Contact history**: Date, times, and duration when this customer contacted your contact center in the past.

4. **Product purchase history**: All the assets purchased by a customer can be populated here. The data is ingested from an external app such as Salesforce or Zendesk that you've integrated with Customer Profiles.

### What is a customer profile in Amazon Connect?

*A customer profile* is a record that stores contact history combined with information about customers, such as account number, additional information, birth date, email, multiple addresses, name, and party type.

After you enable Amazon Connect Customer Profiles, a unique customer profile is created for every contact. This allows you to create a customer profile that has all the information agents need during customer interactions in a single place at no charge.

To access customer profiles in your flows, use the [Customer profiles](#) block. Agents access customer profiles in their agent workspace.

You can use the paid features of Customer Profiles to enrich your customer profiles by ingesting data from external applications. See [pricing](#) for details.

You can also add custom fields and objects to the customer profiles by using the [Amazon Connect Customer Profiles APIs](#).

### How is customer profile data stored?

Amazon Connect stores contact history in unique customer profiles. It parses data ingested from external applications and stores it as customer profile attributes.

Amazon Connect does not replace or update the data in the external application. If a data source is removed, the data from the external application is no longer available in the customer profile for every voice contact.
For information about how customer profile data are secured, see Data protection in Amazon Connect.

For more information about how to access the data that is stored in a customer profile, see Access Customer Profiles in the agent workspace or Use the Customer Profiles API.

Enable Customer Profiles for your instance

Amazon Connect provides pre-built integrations so you can quickly combine customer information from multiple external applications, with contact history from Amazon Connect. This allows you to create a customer profile that has all the information agents need during customer interactions in a single place.

Before you begin

Following is an overview of key concepts and the information that you'll be prompted for during the setup process.

About the customer profiles domain

When you enable Amazon Connect Customer Profiles, you create a customer profiles domain: a container for all data, such as customer profiles, object types, profile keys, and encryption keys. Following are guidelines for creating Customer Profile domains:

- Each Amazon Connect instance can only be associated with one domain.
- You can create multiple domains, but they don't share external application integrations or customer data between each other.
- All the external application integrations you create are at a domain level. All of the Amazon Connect instances associated with a domain inherit the domain's integrations.
- You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain. This isn't recommended, however, because the customer profiles from the earlier domain won't be moved to the new domain.

How do you want to name your customer profiles domain?

When you enable customer profiles, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, CustomerProfiles-ExampleCorp. You can change the friendly name using the API at any time.
Do you want to use a dead-letter queue?

A dead-letter queue is used for reporting errors associated with processing data from external applications.

Amazon AppFlow handles connecting to the external application and moving data from it to Amazon Connect Customer Profiles. Amazon Connect then processes the file.

- If an error occurs during the connection or while transporting the data to Amazon Connect, Amazon AppFlow surfaces the error but it doesn't write the error to the dead-letter queue.

  For example, a processing error could be that the external data didn't match the specified schema or that the format of the external data format isn't correct (currently only JSON is supported).

- If Amazon Connect encounters an error while processing the file, it writes the error to your dead-letter queue. You can look at the queue later and try to reprocess the error.

When you enable Customer Profiles, you have the option of specifying an Amazon SQS queue as your dead-letter queue. If you select this option, add the following resource policy to Amazon SQS so Customer Profiles has permissions to send messages to that queue:

```
{
    "Sid": "Customer Profiles SQS policy",
    "Effect": "Allow",
    "Principal": {
        "Service": "profile.amazonaws.com"
    },
    "Action": "SQS:SendMessage",
    "Resource": "arn:aws:sqs:region:accountID:YourQueueName"
}
```

To prevent a confused deputy security issue, see Amazon Connect Customer Profiles cross-service confused deputy prevention for an example policy to apply.

Step-by-step instructions for creating a dead-letter queue are provided later in this topic, in Enable Customer Profiles, and specify a dead-letter queue and KMS key.
Create a KMS key to be used by Customer Profiles to encrypt data (required)

Note

To maintain access to Customer Profiles APIs, entities using the Customer Profiles profile APIs must have explicit `kms:Decrypt` permissions in their IAM policies. This enables them to utilize `kms:Decrypt` for the KMS key associated with resources retrieved from the API related to Customer Profiles.

When you enable Customer Profiles, you are prompted to create or provide an AWS Key Management Service KMS key. Step-by-step instructions for creating a KMS key are provided later in this topic, in Enable Customer Profiles, and specify a dead-letter queue and KMS key.

All data at rest for Customer Profiles is encrypted under the KMS key you choose. Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

If you choose to set up a KMS key where someone else is the administrator, it must have a policy that allows `kms:GenerateDataKey`, `kms:CreateGrant`, and `kms:Decrypt` permissions to the Customer Profiles service principal. For information about how to change a key policy, see Changing a key policy in the AWS Key Management Service Developer Guide. In addition, to prevent cross-service impersonation, see Cross-service confused deputy prevention for sample policies that you should apply.

Enable Customer Profiles, and specify a dead-letter queue and KMS key

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. In the navigation pane, choose **Customer profiles**.

   The **Customer profiles domain** page lists the applications that are available for integration. In the following image, the page shows no customer profile domains have been enabled.

4. Choose **Enable customer profiles** to get started.

5. At the **Customer profiles enable** page, choose **Create new domain**. Under **Specify a domain**, enter a friendly name that's meaningful to you, such as your organization name, for example, `CustomerProfiles-ExampleCorp`.
6. Under **Specify dead-letter queue**, choose whether to send failed events to a dead-letter queue. This is helpful if you want to get visibility into data that failed to be ingested. It also gives you the option to retry these failed data ingestions in the future.

Following are the steps to create a dead-letter queue:

- On the **Customer profiles enable** page, choose **Create new or select existing SQS queue** and then choose **Create a new Dead Letter Queue**.
A new tab in your browser opens for the Amazon SQS console. Choose **Create queue**.

On the **Create queue** page, choose **Standard**, then assign a name to your queue.
In the Access policy section, choose Advanced.

The Version name, policy ID, and Statement appear. If needed, update this section to give access to only the appropriate roles.

At the end of the Statement section (line 15 in the following image) add a comma after }, and press Enter.
Then copy and paste the following code:

```
{
   "Sid": "Customer Profiles SQS policy",
   "Effect": "Allow",
   "Principal": {
      "Service": "profile.amazonaws.com"
   },
   "Action": "SQS:SendMessage",
   "Resource": "arn:aws:sqs:region:accountID:YourQueueName"
}
```

To replace `region`, `accountID`, and `YourQueueName` with your information, copy and paste the Resource information from line 14.
Choose **Create queue**.

Return to the tab in your browser for the Amazon Connect console, **Customer profiles enable** page. Click or tap in the **Choose existing SQS queue** box to select the queue you just created from the dropdown list.

7. Under **Specify KMS key**, create or enter your own AWS KMS key for encryption. Following are the steps to create your AWS KMS key:
On the **Customer profiles enable** page, choose **Create an AWS KMS key**.

- A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.
On the **Add labels** page, add a name and description for the key, and then choose **Next**.

On the **Define key administrative permissions** page, choose **Next**.

On the **Define key usage permissions** page, choose **Next**.

On the **Review and edit key policy** page, choose **Finish**.

In the following example, the name of the key starts with **bcb6fdd**:

Enable Customer Profiles, and specify a dead-letter queue and KMS key
Return to the tab in your browser for the Amazon Connect console, **Customer profiles enable** page. Click or tap in the **Specify KMS key box** for the key you created to appear in a dropdown list. Choose the key you created.

8. Choose **Submit**. The completed page looks similar to the following image. It shows the name of the customer profiles domain, the dead-letter queue, and the KMS key.

You're done! Amazon Connect Customer Profiles is enabled. Now with every new contact that comes in, Amazon Connect creates a customer profile record. It then tracks the contact history for that phone number (voice) or email address (chat).

Your agents can **create new customer profiles** and view contact records for your customers.
Next steps

1. Make Customer Profiles available through the agent application.
2. Assign agents permissions to access Customer Profiles in the agent application.
3. Integrate with external applications that profile customer profile data (optional).
4. Enable Identity Resolution to identify two or more similar profiles, and consolidate them.

Access Customer Profiles in the agent workspace

After you enable Amazon Connect Customer Profiles, agents can begin interacting with customers and access customer information to provide personalized service. This topic explains how to access the Amazon Connect agent workspace.

Tip

Make sure your agents have Customer profiles permissions in their security profile so they can access Customer Profiles. For more information, see Security profile permissions for Customer Profiles.

Option 1: Use Customer Profiles with the CCP out-of-the-box

Customer Profiles is already embedded alongside the Contact Control Panel (CCP). Your agents can access the CCP, Customer Profiles, and Amazon Connect's Case management all in the same browser window by logging into their Amazon Connect instance and choosing the Agent Workspace button located at the top right corner as shown in the following image.
Note

You can also access the agent workspace by using the following URL:

- **https://instance name.my.connect.aws/agent-app-v2/**

If you access your instance using the **awsapps.com** domain, use the following URL:

- **https://instance name.awsapps.com/connect/agent-app-v2/**

For help finding your instance name, see **Find your Amazon Connect instance name**.

Following is an example of what Customer Profiles looks like in the agent workspace.
Option 2: Embed Customer Profiles into a custom agent workspace

When you embed your Contact Control Panel (CCP), you have the option of showing or hiding the pre-built CCP user interface. For example, you may want to develop a custom agent workspace that has a user interface you design, with customized buttons to accept and reject calls. Or, you may want to embed the pre-built CCP that's included with Amazon Connect into another custom app.

Regardless of whether you display the pre-built CCP user interface, or hide it and build your own, you use the Amazon Connect Streams library to embed the CCP and Customer Profiles into the agent's workspace. This way, Amazon Connect Streams is initialized, and the agent can connect and authenticate to Amazon Connect, and Customer Profiles.

For information about embedding Customer Profiles, see Initialization for CCP, Customer Profiles, and Wisdom.

To build your own widget while using raw data from Customer Profiles, see the Github documentation about how to use the CustomerProfilesJS open source library.
Tip

When you customize the agent's workspace, you determine the URL agents will use to access their agent workspace, and it might very different from the one provided by Amazon Connect. For example, your URL could be https://example-corp.com/agent-support-app.

Use contact attributes to autopopulate customer profiles

By default, Amazon Connect Customer Profiles uses the following values to search for and autopopulate a customer profile in its user interface:

- For voice contacts: Phone number
- For chat contacts: Email

It autopopulates a customer profile by using the Customer Profiles flow block. To customize this behavior, use the following contact attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>profileSearchKey</td>
<td>The name of the attribute you want to use to search for a profile.</td>
<td>User-defined</td>
<td>Not applicable</td>
</tr>
<tr>
<td>profileSearchValue</td>
<td>The value of the key you want to search for, such as customer name or account number.</td>
<td>User-defined</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

For example, to search by email for chat contacts, you can set the profileSearchKey attribute to the _email search key, and provide the email value as the profileSearchValue.

If you have defined custom keys in your profile objects, you can search by those search keys as well. To make sure your custom keys are searchable, see Key definition details.
The following image shows how you might use these attributes in the Set contact attributes block.

Automatically associate a customer profile with a contact

By default, agents need to manually associate a customer profile with a contact based after they've verified the customer's identity. To change this behavior to automatically associate contacts with a profile based on the phone number, see Automatically associate the Contact Record with one profile found using the _phone key.
If multiple profiles match a contact's phone number, the multiple matched profiles are shown to the agent. The agent needs to choose which profile to associate with the contact.

Security profile permissions for Customer Profiles

Contents

- How update permissions for agents
- How update permissions for Flows
- How update permissions for Calculated Attributes
- Issue with permissions: How to assign new permissions

How update permissions for agents

Assign the following **Customer profiles** permissions as needed to the agent's security profile:

- **View**: Enables agents to see the Customer profiles application. They can:
  - View profiles that are autopopulated in the agent app.
  - Search for profiles.
  - View details stored in customer profiles (for example, Name, Address).
  - Associate contact records to profiles, as shown in the following image.

- **Edit**: Enables agents to edit details in the customer profile (for example, change address). They inherit **View** permissions by default.
• **Create**: Enables agents to create and save a new profile. They inherit **View** permissions by default, but don't inherit **Edit** permissions.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

By default, the **Admin** security profile already has permissions to perform all Customer profiles activities.

### How update permissions for Flows

1. Go to the Security profiles console, choose the security profile you would like to edit, or choose **Add new security profile**.

   ![Customer Profiles Table](#)

   **Customer Profiles**  
   This allows various access levels for handling customer profiles.  
<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer profiles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculated Attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Select the **View** permission for Customer Profiles.

   ![Customer Profiles Table](#)

   **Customer Profiles**  
   This allows various access levels for handling customer profiles.  
<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer profiles</td>
<td></td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculated Attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Choose **Save**. You can now navigate to the **User management** section and provide this security profile to the users of your choice.

### How update permissions for Calculated Attributes

1. Go to the Security profiles console, choose the security profile you would like to edit, or choose **Add new security profile**.
2. Select **All** or **View, Edit, Create, and Delete** permission for Calculated Attributes.

3. Choose **Save**. You can now navigate to the **User management** section and provide this security profile to the users of your choice.

**Issue with permissions: How to assign new permissions**

1. In order to update permissions in case of a 403 forbidden call error for any of the backend APIs, navigate to the domain section of the Amazon Connect Customer Profiles console and choose **View details**.
2. Choose **Update Permissions** in the view domain details section.
3. Once this is done, the permissions will be successfully updated and the **Update Permissions** button will no longer be visible in the domain details section. This will mitigate the 403 forbidden error issue and you will be able to make API calls successfully.
Use Identity Resolution to consolidate similar profiles

A similar profile is when two or more profiles are determined to be for the same contact. There can be multiple profiles when customer records are captured across multiple channels and applications for the same customer, and do not share a common unique identifier.

Identity Resolution automatically finds similar profiles and helps you consolidate them. It runs an Identity Resolution Job on a weekly basis, which performs the following steps:

1. Automatic profile matching
2. Automatic merging of similar profiles based on your consolidation criteria
Each time an Identity Resolution Job runs, it displays metrics on the **Customer Profiles** page. The metrics show the number of profiles it reviewed, the number of match groups found, and the number of profiles consolidated.

Additional charges may apply for enabling Identity Resolution. For more information, see Amazon Connect pricing.

**Enable Identity Resolution for your Customer Profiles domain**

When you enable Identity Resolution you specify the following information:

- When the Identity Resolution Job should run on a weekly basis. By default, it runs Saturdays at 12AM UTC.
- The Amazon S3 bucket where the Identity Resolution Job should write the results of the automatic profile matching process. If you don't have an S3 bucket, you'll have the option to create one during the enablement process.

You can query the Amazon S3 bucket or use the [GetMatches API](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/) to filter results based on confidence scores.
To enable Identity Resolution

1. You must have a Customer Profiles domain enabled for your instance. For instructions, see Enable Customer Profiles for your instance.
2. In the navigation pane, choose Customer profiles.
3. In the Identity Resolution section, choose Enable Identity Resolution.
4. In the Identity Resolution pop-up box, choose Enable Identity Resolution.

Note
After you enable Identity Resolution you'll see the option to create consolidation criteria for the optional auto-merging process.
5. On the **Enable Identity Resolution** page, specify the date and time when you want the Identity Resolution Job to run.

6. If you want to review the matched profile IDs from an Amazon S3 bucket, select **Write profile ID matches to Amazon S3**. Otherwise, you can use the [GetMatches] API to review matching profiles.

   - Specify the Amazon S3 bucket where the Identity Resolution Job should write the profile matches.
We recommend applying a policy to prevent a confused deputy security issue. For more information and a sample policy, see Amazon Connect Customer Profiles cross-service confused deputy prevention.

7. When done, choose Enable Identity Resolution. Both rule-based matching and ML-based matching are enabled after you enable Identity Resolution. You can disable one of them or both from the Identity Resolution page. For more information, see Disable Identity Resolution.

8. Rule-based matching for Identity Resolution:
   a. After you enable the rule-based matching with a new domain the matching will start immediately if you set up an integration and the integration is running.
   b. After you enable the rule-based matching with an existing domain, the matching process will start within one hour.

9. ML-based matching for Identity Resolution:
   a. After you enable Identity Resolution the Identity Resolution Job runs for the first time within 24 hours.

   Note
   Before running an Identity Resolution Job for the first time on a new Customer Profiles domain, we recommend checking your profile metrics to make sure that profiles have been created. Otherwise, there won't be any matching results.

   b. You may want to set up consolidation criteria for auto-merging matching profiles. If so, see Set up consolidation criteria for Identity Resolution.

Machine learning for Identity Resolution

Contents

- How machine learning Identity Resolution works
- Set up machine learning for Identity Resolution
- Set up consolidation criteria for Identity Resolution
How machine learning Identity Resolution works

This topic describes how Identity Resolution performs automatic profile matching, and if set up, how it automatically merges similar profiles.

Automatic profile matching

To identify similar profiles, Identity Resolution uses machine learning to review the following Personal Identifiable Information (PII) attributes in each profile:

- Name: All names are reviewed for similarity, including first name, middle name, and last name.
- Email: All email addresses are reviewed for similarity, including personal email and business email. They are not case sensitive.
- Phone number: All phone numbers and formats are reviewed for similarity, including home phone, mobile phone, and business phone.
- Address: All address types and format are reviewed for similarity, including business address, mailing address, shipping address, and billing address.
- Date of birth: All birth dates and formats are reviewed for similarity.

It uses this information to create match groups of similar profiles.

Match groups

A match group consists of all similar profiles which represents a customer. Each match group contains the following information:

- A match ID, which uniquely identifies the group of two or more similar profiles that represent a contact
- The number of profile IDs in the match group
- A confidence score associated with the match group

Confidence scores

After the auto-matching process runs, you can query the S3 bucket or use the GetMatches API to filter results based on confidence scores. For example, you can filter out high confidence matches for a further review.
A confidence score is a number between 0 and 1 that represents the confidence level of assigning profiles to a match group. A score of 1 likely indicates an exact match.

**Automatic merging of similar profiles**

After the profiles are matched, the Identity Resolution Job can optionally merge similar profiles based on your criteria. If you delete or update criteria, the updated criteria is applied to similar profiles in the next run.

> **Important**
> You cannot undo the consolidation process. We strongly recommend using the [GetAutoMergingPreview](#) API to do a dry run of the automatic merging process before running the Identity Resolution Job.

### How the auto-merging process works

- **All selected attributes in a consolidation criteria are connected with AND criteria with exact value comparison before merging.**
  - For example, when multiple attributes are specified in the criteria, such as `email address` and `phone number`, then all similar profiles in a match group that have the exact same value of `email address` and `phone number` are merged.
  
  If one or more of the similar profiles in a match group have a different value or missing value for one or more of the attributes in a criteria, the similar profiles are merged.

  For example, one match group may be five similar profiles out of which three profiles are consolidated, because these three profiles meet the criteria. The other two profiles are not merged, because they do not meet the criteria.

- **Multiple criteria are evaluated in the order of priority starting with Criteria 1.**
  - The sequence in which consolidation criteria are applied. It starts with Criteria 1 as the highest priority to Criteria 10 as the lowest priority.
  
  After the Identity Resolution Job applies one criteria, it applies the next criteria to the consolidated profiles and the remaining similar profiles in a match group.

  You can have a maximum of 10 consolidation criteria.

- **Each criteria runs independently and operates as an OR with other criteria.**
• When you have multiple criteria, each criteria is applied individually and in the sequence of priority order before the Identity Resolution Job moves on to the next criteria.

• All criteria is applied in the sequence in which you listed them. It doesn't matter whether the criteria fails or succeeds to consolidate similar profiles in a match group.

• **By default, profile conflicts are managed by recency.**

  • When two or more similar profiles in a match group meet a consolidation criteria, the resulting consolidated profile is created by comparing each value of the profile attributes constituent similar profiles.

  • Each attribute may have an exact match in value. In this case, any value may be selected for that attribute.

  • If there is a conflict between values of two or more constituent similar profiles, the most recently updated attribute is chosen.

    For example, if Jane Doe has three different values in the Address attribute of the constituent similar profiles, Identity Resolution picks the most recent addressed to create the unified profile.

  • By default, the **Last updated timestamp** is used to determine the record that was most recently updated.

• **Profile conflicts are managed by source object type and recency.**

  • You can also change default behavior of conflict resolution to choose a similar constituent profile from a specific source as the source of truth to inform conflict resolution.

  • If you want to specify a data source to use for profile conflicts, you can choose one of your object types as a data source if you select **Source with last updated timestamp**.

  • The most recently updated record from the specified object type is used for resolving profile conflicts.

• **Last updated timestamp identifies which record was most recently updated.**

  • The timestamp attribute associated with the source record's object type is used to identify which record was most recently updated.

  • If the timestamp attribute is not available for the object type, the timestamp on which the record was ingested into your Customer Profiles domain is used.

  • If you have custom object types, you need to add timestamps. See [Missing timestamp for profile conflicts](#) for more information.

• **Consolidation is a one-way process and cannot be undone.**
• Choose your criteria carefully before starting the consolidation process. For more information, see Tips for creating strong criteria.

• Use the GetAutoMergingPreview API to test the auto-merging settings of your Identity Resolution without merging your data.

For an example that shows how criteria is applied, see Example: How sample criteria are applied.

**Set up machine learning for Identity Resolution**

**Edit machine learning matching run schedule**

![Edit run schedule](image)

- **Run schedule**
  - Choose the day and time to start Identity Resolution's weekly run.
  - Saturday at 12:00 AM

- **Use 24 hour format. All times in UTC.**

- **Local time for the selected UTC run schedule**
  - Saturday at 12:00 AM
Edit machine learning merge matches

You can merge profile matches to consolidate similar profiles. You cannot revert profiles after they are merged.

**Merge matches**
Define when to merge profile matches found by machine learning matching.

**Merge rules**
You can define rules for merging profile matches by comparing attribute values. Profiles must match all attributes within the rule exactly to be consolidated.

---

**Rule 1**
Attributes

- **AccountNumber**
- **AdditionalInformation**
- **Address.Address1**

Tips for creating strong rules

- We recommend defining rules that can uniquely identify a profile, such as Email or Account number.
- Avoid generic rules, such as Last name and First name attributes, which are likely to identify profiles that are not unique. Learn more.

**Rule 2**
Attributes

- **Address.City**
- **Address.PostalCode**
- **FirstName**

Tips for creating strong rules

- We recommend defining rules that can uniquely identify a profile, such as Email or Account number.
- Avoid generic rules, such as Last name and First name attributes, which are likely to identify profiles that are not unique. Learn more.
Edit machine learning match location

Set up consolidation criteria for Identity Resolution

Note
You must enable Identity Resolution in order to access the option to create consolidation criteria using the Amazon Connect admin console.

When similar profiles are detected by an Identity Resolution Job, the process can automatically merge them into a unified profile based on consolidation criteria that you specify.

The attributes that you select are compared across all similar profiles in a match group for exact match. For example, if you specify email as an attribute in the criteria, then all similar profiles in a match group that have exact same value of email address are merged into a unified profile.

Tip
If you want to set up your own merging logic, use the MergeProfiles API.
Limits

You can select any attribute from the standard profile to compare similar profiles. For example, you might choose phone number, email address, and name, as well as custom attributes.

You can specify up to:

- 10 consolidation criteria
- 20 attributes per criteria

Tips for creating strong criteria

To improve the targeting of unique profiles and to avoid consolidating profiles that are not duplicates, we recommend the following steps:

- Select attributes that can uniquely identify a customer and are not likely to be the same across customers, such as an account number or a form of government ID.
- Avoid single attribute criteria. Select multiple attributes to create a combination of attributes to improve targeting. For example:
  - **Phone number** with **First name, Middle name, Last name** is stronger criteria than
    - **Phone number** alone, or
    - The combination of **First name, Middle, name, Last name** alone
- Select all attributes within a specific attribute group, when applicable. For example, if you want to use name, select all the related name attributes: **First name, Middle name, Last name**. If you want to use business address, select all the related business address attributes.
- Include one of the following attributes likely to uniquely identify a customer in combination with other attributes in the criteria:
  - Account number
  - Phone number
  - Email

How to set up auto-merging criteria

Before setting up your consolidation criteria for automatic merging, or auto-merging, we recommend reviewing [How the auto-merging process works](#).
1. After you enable Identity Resolution, on the **Identity Resolution** page you'll have the option of setting up auto-merging criteria. Choose **Create consolidation criteria**.

2. If you receive a **Missing timestamp** dialog box, we recommend adding new timestamp attributes to your custom object types before continuing. See [Missing timestamp for profile conflicts](#).

3. In the **Profile conflicts** section, choose how profile conflicts should be resolved when two or more records have conflicts.

4. In the **Consolidation criteria** section, create one or more criteria. We recommend including at least two or more attributes per criteria.

### Missing timestamp for profile conflicts

The **Missing timestamp** message is displayed if you have custom object type mappings.

Use the [PutProfileObjectType](#) API to add the following new attributes to your custom object type:

- Fields.sourceLastUpdatedTimestamp
- sourceLastUpdatedTimestampFormat

If the timestamp attribute is not specified, you can continue to create consolidation criteria, however, a default timestamp of when the records were ingested into Customer Profiles is used. We recommend adding the new attributes before creating your consolidation criteria.

If you have already defined a custom object type and want to update your custom object type, we run a scheduled backfill every week to update your existing profiles with the Fields.sourceLastUpdatedTimestamp. To opt in to the scheduled backfill:

1. Update your custom profile object type by using the [PutProfileObjectType](#) API.

2. After you update your custom profile object type, open an [AWS Support ticket](#) and we’ll schedule the backfill for you. The scheduled backfill runs until end of February 2022.

Alternatively, you can delete and then re-create the ingestion/connector you have for your domain that uses the custom object type. All of your data will be re-ingested using your updated object type and Fields.sourceLastUpdatedTimestamp will be parsed from it.
Example: How sample criteria are applied

In this example there are three criteria:

- **Resolve profile conflicts** is set to **Use last updated timestamp**. This means when two fields have conflicting values, Identity Resolution is going to use the last updated timestamp to determine which value to use.

- Criteria 1:
  - First name, Last name
  - Email

- Criteria 2:
  - Phone number

These criteria are applied to the following profiles:

- **Profile A**
  - John Doe [last updated 05:00a]
  - doefamily@anyemail.com [last updated 05:00a]
  - 555-555-5555 [last updated 07:00a]

- **Profile B**
  - John Doe [last updated 04:00a]
  - doefamily@anyemail.com [last updated 06:00a]
  - 555-555-5556 [last updated 04:00a]

- **Profile C**
  - Jane Doe [last updated 06:00a]
  - doefamily@anyemail.com [last updated 07:00a]
  - 555-555-5555 [last updated 06:00a]

Following are the results when Criteria 1 is applied:

- Profile A and B are merged = Profile AB

This results in ProfileAB, which looks like the following:
• John Doe [last updated 05:00a]
• doefamily@anyemail.com [last updated 07:00a]
• 555-555-5555 [last updated 06:00a]

Because there's a conflict between the phone numbers, Identity Resolution uses the last timestamp to choose the 555-555-555 number.

Next, Criteria 2 is applied. Following are the results:

• Profile AB and C are merged = Profile ABC

This results in Profile ABC, which looks like the following:

• Jane Doe [last updated 06:00a]
• doefamily@anyemail.com [last updated 07:00a]
• 555-555-5555 [last updated 07:00a]

Identity Resolution uses the First name, Last name, and Email from Profile C because they have the most recent timestamps.

**Rule-based matching for Identity Resolution**

**Contents**

- [How rule-based Identity Resolution works](#)
- [Set up rule-based matching for Identity Resolution](#)
- [Set up matching rules for rule-based Identity Resolution](#)

**How rule-based Identity Resolution works**

This topic describes how rule-based Identity Resolution performs automatic profile matching and how it automatically merges similar profiles.

**Automatic profile matching**

To identify similar profiles, the rule-based Identity Resolution uses a list of matching rule attributes to match each profile. Up to 15 MatchingRule attributes are supported in the MatchingRules.
Matching rules

The following is a list of the MatchingRule attributes that can be used. You can configure up to 15 matching rule levels. For each matching rule, you can use the following Personal Identifiable Information (PII) attributes in each profile:

- **AccountNumber**
- **Address.Address**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.City**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.Country**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.County**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.PostalCode**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.State**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **Address.Province**: All addresses specified in the Attribute Type Selector are reviewed for similarity, including Address, BusinessAddress, MaillingAddress, and ShippingAddress
- **PhoneNumber**: The phone numbers specified in the Attribute Type Selector are reviewed for similarity, including PhoneNumber, HomePhoneNumber, and MobilePhoneNumber.
- **EmailAddress**: All email addresses specified in the Attribute Type Selector are reviewed for similarity, including EmailAddress, BusinessEmailAddress, and PersonalEmailAddress
- **BirthDate**
- **BusinessName**
- **FirstName**
- **LastName**
- **MiddleName**
- **Gender**
- **Any customized profile attributes with the Attributes prefix**
Matching rules are processed by priority. For example, the first rule should be the most optimized rule you want to define and should be used to achieve the most accurate result.

**Attribute Type Selector**

The Attribute Types Selector holds vital configuration information for rule-based identity resolution, facilitating profile matching. This allows you to fine-tune the comparison of profiles across attribute types and select the key attributes for matching within each type. Within this feature, you have the flexibility to configure three distinct attribute types, enabling precise control over the matching process.

- **Email type**
  - You can choose from EmailAddress, BusinessEmailAddress, and PersonalEmailAddress
- **PhoneNumber type**
  - You can choose from PhoneNumberNumber, HomePhoneNumber, and MobilePhoneNumber
- **Address type**
  - You can choose from Address, BusinessAddress, MaillingAddress, and ShippingAddress

You can either choose **ONE_TO_ONE** or **MANY_TO_MANY** as the AttributeMatchingModel. When choosing **MANY_TO_MANY**, the system can match attributes across the sub-types of an attribute type. For example, if the value of the EmailAddress field of Profile A and the value of BusinessEmailAddress field of Profile B matches, the two profiles are matched on the EmailAddress type. When choosing **ONE_TO_ONE**, the system can only match if the sub-types are exact matches. For example, only when the value of the EmailAddress field of Profile A and the value of the EmailAddress field of Profile B matches, the two profiles are matched on the EmailAddress type.

**Max allowed rule level for matching**

You can configure the max rule level you want to use to match similar profiles. For example, if your max allowed rule level for matching is 5, the system will not find similar profiles using the rule level 6.

**Match groups**

A match group consists of all similar profiles which represent a customer. Each match group contains the following information:

- A match ID, which uniquely identifies the group of two or more similar profiles that represent a contact
- The number of profile IDs in the match group

**Match status**

- **PENDING**

  The first status after the configuration of a rule-based Matching rule. If it is an existing domain, the rule-based Identity Resolution waits 1 hour before creating the matching rule. If it is a new domain, the system will skip the **PENDING** stage.

- **IN_PROGRESS**

  The system is creating the rule-based Matching rule. Under this status, the system is evaluating the existing data and you can no longer change the rule-based matching configuration.

- **ACTIVE**

  The rule is ready to use. You can change the rule a day after the status is in an **ACTIVE** state.

**How the auto-matching process works**

After you create a new Amazon Connect Customer Profiles domain with the rule-based matching rule, the rule-based Identity Resolution will match similar profiles based on the rule you specified while you are ingesting the profiles. If you update the configuration of the rule-based matching, Customer Profiles will start to re-evaluate the profiles in your domain using the new configuration in an hour.

If you are enabling the rule-based matching with an existing domain, the system will move to a **PENDING** state and will start to evaluate the existing profiles in your domain using the new configuration in an hour. The time it takes to finish evaluating profiles is dependant on how many profiles exist.

- **By default, the default rule will be applied if no custom rule specified.**
  
  - Amazon Connect Customer Profiles provides a default matching rule if you do not provide a custom matching rule. You can check the custom matching rule here.

- **All the records will go through the rule-based matching rules.**
  
  - The system assesses each matching rule level until a match is identified or until the maximum allowed rule level for matching is reached. The evaluation process commences at rule level 1, where the record is analyzed. If no matching group is discovered, the system proceeds to...
evaluate the subsequent rule levels, searching for a match group until either a match is found or the maximum allowed rule level for matching is reached.

- **All attributes in a single matching rule level are connected using an AND relationship**

  - When multiple attributes are present within a single rule level, they are interconnected by an AND relationship. During profile matching, all attribute values must align for profiles to be assigned to the same match group. For example, only when the values of all attributes are identical, profiles are considered as matches and grouped together for further processing.

- **All attributes in an attribute type selector are connected with an OR relationship**

  - When specifying attributes within the attribute type selector, attributes of the same type are linked through an OR relationship. For instance, consider the PhoneNumber Type where HomePhoneNumber and BusinessPhoneNumber are utilized. In this scenario, two profiles can be matched if either their HomePhoneNumber or BusinessPhoneNumber aligns. Consequently, the matching process allows for flexible matches based on either home or business phone numbers.

- **The match result is eventually optimized.**

  - Due to the near real-time nature of profile matching in the system, there is a possibility that a match group for your profile may be found at a lower (less optimized) rule level. Nevertheless, if a match is available at a higher (more optimized) rule level, the system will assign the profile to that particular group.

---

**Note**

When Identity Resolution performs rule-based matching, the order in which the rules that you have configured will be processed is dependant on how the data is ingested. For example, if you configure rules 1 and 2, rule 2 might be processed before rule 1. The processing order might change, but the end result will always be the same.

---

**Automatic merging of similar profiles**

After the profiles are matched, the Identity Resolution Job can optionally merge similar profiles based on the `MaxAllowedRuleLevelForMerging` you specify in the rule-based matching configuration.
Important

You cannot undo the consolidation process. It is recommended to turn on matching only first to evaluate the match result using the ListMatches and GetSimilarProfiles APIs. You can turn on merging by setting the `MaxAllowedRuleLevelForMerging` using the `UpdateDomain` API.

Set up rule-based matching for Identity Resolution
Edit rule-based matching attribute types

You can select the attribute types, such as email or phone number, to use to find profile matches. For example, if your business wants to match on multiple types of email addresses, you can choose many to many to match across profiles and the attribute type used by your business.

**Match across profiles**
You can compare profiles with the same attribute type across multiple attribute types.

- **Compare attribute types**
  - One to one
    Use this for more precise matching to compare on the same attribute type. For example, profile A (personal phone) and profile B (personal phone).
  - Many to many
    Use this for broader matching to compare across multiple attribute types. For example profile A (personal phone) with all attribute types of profile B (mobile phone, personal phone, business phone).

- **Attribute types**
Select the attribute type you want to use for matching profiles.

  - **Email type**
    Select the email attributes relevant to your data.
    - Email (unspecified)
    - Personal email
    - Business email

  - **Phone number type**
    Select the phone number attributes relevant to your data.
    - Phone (unspecified)
    - Home phone
    - Mobile phone
    - Business phone

  - **Address number type**
    Select the address attributes relevant to your data.
    - Address (unspecified)
    - Mailing address
    - Shipping address
    - Business address
Edit rule-based matching rules

Your data will be evaluated against a set of rules to find exact matches for Rule-based matching. You can customize how matches are found by selecting attribute values to compare for each rule.

### Rule 1
Attributes
- Address.Address
- Address.City
- Address.Country

Show more chosen options (+6)
You can add up to 4 more attributes.

### Rule 2
Attributes
- Address.Address
- Address.City
- Address.Country

Show more chosen options (+7)
You can add up to 5 more attributes.

### Rule 3
Attributes
- Address.Address
- Address.City
- Address.Country

Show more chosen options (+7)
You can add up to 5 more attributes.
Reset rule-based matching rules

All changes made to the matching rules will be removed and the default rules will be applied. Learn more

Edit rule-based matching merge rules

You can merge profile matches to consolidate similar profiles. You cannot revert profiles after they are merged.

Merge matches
Define when to merge profile matches found by rule-based learning matching.

Merge matches
Use merge matches to automatically consolidate profile matches into a single profile.

Rule priority for merging
Choose a rule to define the minimum rule level for merging profile matches. Matches that meet this rule and higher priority rules will be merged.

Advanced merge options

You cannot revert profiles after they are merged.
Edit rule-based match location

Set up matching rules for rule-based Identity Resolution

Limits

You can select any attribute from the standard profile to compare similar profiles. For example, you might choose phone number, email address, and name, as well as custom attributes.

You can create a rule-based matching rule with the following limitations:

- 15 rule levels
- Each rule level can contain up to 15 profile attributes

Tips

To improve the targeting of unique profiles and to avoid consolidating profiles that are not duplicates, the following tips are recommended:

- Include at least one high cardinality attribute that can uniquely identify a customer and that is not likely to be the same across customers, such as a phone number, an email address or an account number.
- Avoid using profile attributes that can belong to different identities without a high cardinality attribute.
• **Phone number** with **First name, Last name** is a stronger rule than the combination of **First name, Last name** alone.

• If at one rule level, all of the profile attributes of that rule are low cardinality attributes (the attribute that can belong to more than 500 different profiles), the system will not attempt to match the profile. You will receive the following SQS message in your DLQ if you setup one during the domain creation:

  • All attributes at rule level x are associated with more than 500 records.

• Always enable **Match only** first, check the match results, and only enable the merging by setting the **MaxAllowedRuleLevelForMerging** if you are satisfied with the match results.

**Resolve Profile Conflicts for profile merging**

You can define which record to use when the value of an attribute from two or more similar profiles is different, such as conflicting address records.

**Last updated timestamp**

By default, profile conflicts are managed by recency. When there is a conflict between the values of two or more similar profiles, the most recently updated attribute will be chosen.

**Source with last updated timestamp**

Allows you to prioritize records from a specific object type as your data source for managing profile conflicts. When there is a conflict between the values of two or more similar profiles, the most recently updated attribute from the specified object type will be chosen.

If a timestamp is not specified in your object type, the date the record was ingested into Customer Profiles will be used. Source with last updated timestamp is unavailable when you don't have any integrations set up. When you add an integration, your object types will be available as a source for this option.

**Missing timestamp for profile conflicts**

The Missing timestamp message is displayed if you have custom object type mappings.

Use the [PutProfileObjectType](#) API to add the following new attributes to your custom object type:

• **Fields.sourceLastUpdatedTimestamp**
• `sourceLastUpdatedTimestampFormat`

If the timestamp attribute is not specified, you can continue to create consolidation criteria, however, a default timestamp of when the records were ingested into Customer Profiles is used. It is recommended to add the new attributes before creating your consolidation criteria.

If you have already defined a custom object type and want to update your custom object type, we run a scheduled backfill every week to update your existing profiles with the `Fields.sourceLastUpdatedTimestamp`. To opt in to the scheduled backfill, use the following steps:

1. Update your custom profile object type by using the `PutProfileObjectType` API.
2. After you update your custom profile object type, open an [AWS Support ticket](https://aws.amazon.com/support/). 
3. AWS will schedule the backfill on your behalf. The scheduled backfill runs until end of February 2022.

Alternatively, you can delete and then re-create the ingestion/connector you have for your domain that uses the custom object type. All of your data will be re-ingested using your updated object type and `Fields.sourceLastUpdatedTimestamp` will be parsed from it.

**Example: How matching works**

**Example for ONE_TO_ONE**

You can choose ONE_TO_ONE as the `AttributeMatchingModel`. When choosing ONE_TO_ONE the system can only match if the sub-types are exact matches.

**For example:**

You are using the `EmailAddress` and `BusinessEmailAddress` to represent the `EmailAddress` types. The `AttributeMatchingModel` is ONE_TO_ONE.

**Your matching rule is:**

```
Rule Level 1: EmailAddress, LastName, FirstName
Rule Level 2: AccountNumber
```
Profile A:
EmailAddress: 1@email.com
BusinessEmailAddress: john@company.com
LastName: Doe
FirstName: John
AccountNumber: account1234

Profile B:
EmailAddress: 2@email.com
BusinessEmailAddress: john@company.com
LastName: Doe
FirstName: John
AccountNumber: account1234

The Profile A and Profile B matches at rule level 1 since the EmailAddress type, LastName, and FirstName match.

**Example for MANT_TO_MANY**

You can choose MANT_TO_MANY as the AttributeMatchingModel. When choosing MANT_TO_MANY, the system can match attributes across the sub-types of an attribute type.

**For example:**

You are using the EmailAddress and BusinessEmailAddress to represent the EmailAddress types. The AttributeMatchingModel is MANT_TO_MANY.

**Your matching rule is:**

Rule Level 1: EmailAddress, LastName, FirstName
Rule Level 2: AccountNumber
Profile B:
EmailAddress: 2@email.com
BusinessEmailAddress: 1@email.com (match with Profile A’s EmailAddress)
LastName: Doe
FirstName: John
AccountNumber: account1234

The Profile A and Profile B matches at rule level 1 since the EmailAddress type, LastName, and FirstName match.

Identity Resolution metrics

Whenever Identity Resolution matches or merges profiles, metrics about the process are displayed on the Customer Profiles dashboard. You can review metric for the pass week on the Identity Resolution summary page.

The following metrics are generated each time the Identity Resolution Job runs:

- **Match groups found**: The number of match groups that were found.
  - Available for both ML-based and rule-based Identity Resolution.
- **Profiles Merged**: The number of profiles that were merged.
  - Available for both ML-based and rule-based Identity Resolution.
- **Match Group by rule**: The number of match group that were created by each rule level.
  - Only available for rule-based Identity Resolution.
Identity Resolution

Identity Resolution settings (2)

- Name
  - Rule-based resolution
    - Find matches: Pending
    - Merge matches: Inactive
  - Machine learning resolution
    - Find matches: Active
    - Merge matches: Inactive

Last updated:
- March 23, 2023, 18:20 (UTC)

Match groups found
March 18, 2023, 00:00 (UTC) - March 23, 2023, 18:20 (UTC)

Profiles merged
March 18, 2023, 00:00 (UTC) - March 23, 2023, 18:20 (UTC)

Match groups by rule (3)
March 18, 2023, 00:00 (UTC) - March 23, 2023, 18:20 (UTC)
Disable Identity Resolution

Disable machine learning-based

You can disable machine learning-based matching when you no longer want it to automatically find similar profiles. If you have consolidation criteria, all your criteria will be deleted and your profiles will no longer be automatically consolidated. Profiles that have already been consolidated will remain consolidated.

Disable rule-based matching

You can disable rule-based matching when you no longer want it to automatically find similar profiles. If you have a custom matching rule, the matching rule will be deleted and your profiles will no longer be automatically consolidated. Profiles that have already been consolidated will remain consolidated.

Integrate external applications with Customer Profiles

Amazon Connect provides a set of pre-built integrations powered by Amazon AppFlow and Amazon EventBridge. After you enable Amazon Connect Customer Profiles, you can use these integrations to combine information from external applications such as Salesforce or Zendesk, with contact history from Amazon Connect. This creates a customer profile that has all the information agents need during customer interactions in a single place.
You can also use Customer Profiles in Amazon AppFlow. Amazon AppFlow supports CustomerProfiles as a destination. You can use Amazon AppFlow APIs to send data into Customer Profiles using CustomerProfiles as the destination name.

Before you begin, make sure you are using a customer managed key. For more information about configuring KMS keys, see Create a KMS key to be used by Customer Profiles to encrypt data (required).

**Set up integrations**

You can setup an integration using either featured applications in Amazon Connect or external applications using Amazon AppFlow by choosing the method that best fits your use-case below. For more detailed information on the integration of ServiceNow and Slack, see the blog post Combine data from multiple sources using Amazon AppFlow and build a unified Amazon Connect Customer profile for contact center agents.

Contents

- Set up integration for featured applications in Amazon Connect
- Set up integration for external applications using Amazon AppFlow
- Delete/stop Customer Profiles integrations

**Set up integration for featured applications in Amazon Connect**

These integrations use Amazon Connect featured applications to provide periodic updates to Amazon Connect Customer Profiles.

**Before you begin**

**Bulk ingestion of data**

When you set up your integration, you are prompted to enter a date how far back you want to go to ingest data. If you choose a date that is more than two months ago, Customer Profiles automatically enables bulk ingestion by creating multiple flows. It does this so you don't have to calculate how many flows you need to ingest data.

When automatic bulk ingestion is enabled, Customer Profiles does the following:

- Sets the batch size to two months.
- Retries on transient failures up to three times before failing.
You can use the `CreateIntegrationWorkflowRequest` API to call your own batch size.

**Why am I asked to select or create an IAM role?**

For Salesforce, Marketo, and ServiceNow, Customer Profiles helps improve the historical ingestion of these sources by using your IAM role to create several workflows to ingest your data quickly and efficiently.

For these sources, if you select more than 60 days back in the **Date for importing records** date picker, you will be prompted to create a new IAM role or select an existing one. This role allows Customer Profiles to manage your integration. It provides Customer Profiles with the necessary permissions to update and create a workflow to ingest your data. After the workflow is complete, Customer Profiles creates a standard, continuous integration that ingests your new data as it is updated in your source.

The role created in the console is only useable by the domain it was created on. This is because Amazon Connect limits the access of the role to only the KMS key used by the domain.

For more information, see [Grant least privilege access to your Customer Profiles execution role](#).

**Grant least privilege access to your Customer Profiles execution role**

If you want to create your own IAM role, we recommend using the permissions shown in the following code to limit the role to the least permissions needed. Use the snippet below to create your role manually. Use your own KMS key and specify your Region where needed.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Condition": {
            "ForAnyValue:StringEquals": {
               "aws:RequestTag/awsOwningService": "customer-profiles-integration-workflow"
            }
         },
         "Action": [
            "appflow:CreateFlow",
            "appflow:TagResource",
            "profile:TagResource",
            "profile:PutIntegration"
         ]
      }
   ]
}
```
"Resource": "*",
"Effect": "Allow",
"Sid": "CreateFlowResources"
},
{
    "Action": [
        "appflow:UseConnectorProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "UseConnectorResources"
},
{
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:ResourceTag/awsOwningService": "customer-profiles-integration-workflow"
        }
    },
    "Action": [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DeleteFlow",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "profile:DeleteIntegration"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AccessFlowResources"
},
{
    "Action": [
        "kms:CreateGrant",
        "kms:ListGrants"
    ],
    "Resource": "{{YourKMSKeyConsumedByTheDomain}}",
    "Condition": {
        "kms:ViaService": [
            "appflow.{{region}}.amazonaws.com"
        ]
    }
}
Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose Flow details to learn more about what's gone wrong.

You may need to delete the configuration and re-connect to the external application.

Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk

To provide periodic updates to Amazon Connect Customer Profiles, you can integrate with Salesforce, ServiceNow, Marketo, or Zendesk using Amazon AppFlow. You first set up the connection in Amazon Connect and the application of your choice, and then verify the integration.
Set up the connection in Amazon Connect and Salesforce, ServiceNow, Marketo, or Zendesk

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

![Amazon Connect virtual contact center instances](image)

3. In the navigation pane, choose Customer profiles.

4. On the Customer profiles configuration page, choose Add integration, as shown in the following image.

![Customer profiles configuration](image)

5. On the Select data source page, choose which external application you want to get customer profiles data from. You can view the integration requirements to better understand the connection requirements needed for your application.
6. On the **Establish connection** page, choose one of the following:

   - **Use existing connection**: This allows you to reuse existing Amazon AppFlow resources you may have created in your AWS account.
   - **Create new connection**: Enter the information required by the external application.

7. On the **Integration options** page, choose which source objects you want to ingest and select their object type.

   Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to
the standard objects in Customer Profiles. You can also use the object mappings that you’ve created from the `PutProfileObjectType`. When adding or creating the Salesforce integration for the user created data mapping, you need to specify the specific data mapping, otherwise it will choose the Salesforce default data mapping for object type. You can create your data mapping and use it when setting up a featured data connector.

8. For the **Ingestion start date**, Customer Profiles starts ingesting records created after this date. By default, the date for importing records is set at 30 days prior.

9. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Create integration**.
10. After the integration is set up, back on the Customer profiles configuration page, choose View objects to see what data is being batched and sent. Currently, this process ingests records that were created or modified in the last 30 days.

Set up integration for Segment

To provide periodic updates to Amazon Connect Customer Profiles, you can integrate with Segment using Amazon AppFlow. You first set up the connection in Amazon Connect and Segment, and then verify the Segment integration.

Set up the connection in Amazon Connect and Segment

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

![Amazon Connect virtual contact center instances](image)

In the navigation pane, choose Customer profiles.


![Customer profiles configuration](image)

5. On the Select data source page, choose Segment. Review the application requirements that are listed on the Select application page.
6. On the **Establish connection** page, choose one of the following:

- **Use existing connection**: This allows you to reuse existing Amazon EventBridge resources that you may have created in your AWS account.

- **Create new connection**: Enter the information required by the external application.
- **Connection name**: Provide a name for your connection. The connection name is referenced by integrations that use this connection.

- **Connection URL**: Enter your application connection URL. This URL is used for deep-linking into the objects created in your external application. The connection URL is the Segment workspace URL available on the application website.

  To find your workspace URL:

  1. Log in to your segment.com account.
  2. Go to **Settings, General settings**.
  3. Copy the URL from your browser.

7. Customer Profiles uses Amazon EventBridge for integrations with Segment. On the **Source setup** page, copy your AWS account ID to your clipboard, and then choose **Log in to Segment** to configure Amazon EventBridge.

8. Use the following instructions to set up Segment:
a. Log in to Segment.

b. In your application, select a source to set up the destination to Amazon EventBridge.

c. Paste in your AWS account ID and select your AWS Region.

d. Toggle ON, to activate your partner event source.

9. Go to Event Tester, and send a test event to complete activating your partner event source.

10. **Client ID**: This is a string that uniquely distinguishes the client in your external application. This client ID is the Source Name available on the application website. You use the ID that you specify to identify the client that you want Customer Profiles to ingest your objects from.

To find your source ID:

1. Go to Sources, and choose a source.

2. Go to Settings, API Keys.

3. Copy your Source ID.

After you set up the event source destination, return to the Customer Profiles console and paste the Client ID.

11. You will see an alert that indicates Amazon Connect has successfully connected with Segment.

12. On the **Integration options** page, choose which source objects you want to ingest and select their object type.

Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to the standard objects in Customer Profiles. You can also use the object mappings that you’ve created from the **PutProfileObjectType**.
13. For the **Ingestion start date**, Customer Profiles starts ingesting records created after the integration is added.

![Object type Info](image)

**Note**

If you need historical records, you can use Amazon S3 as an integration source to import them.

14. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Add integration**.

15. After the integration is set up, back on the **Customer profiles configuration** page, the **Integrations** page displays which integrations are currently set up. The **Last run** and **Integration health** are not currently available for this type of integration.
To see what data is being sent, choose the integration and then choose View objects.

Verify your Segment integration

To perform this step you need the following prerequisites:

- Access to your Segment workspace.
- Access to the Amazon Connect Contact Control Panel.

To verify your Segment integration

1. Go to your Segment workspace dashboard and choose Destinations.
2. You will see a list of destinations where that Segment sends data. Choose the EventBridge destination for Customer Profiles.

3. Choose the **Event Tester** tab. From this page you will send a test event to Customer Profiles. The event is ingested and turned into a customer profile that you can view in the Amazon Connect agent application.
4. Select **Identify** as the event type, and select **Event Builder** as your input method.

5. You can specify a **User ID** and some traits. Agents can search for these traits in the agent application.

6. Choose **Send Event**.

7. The event delivery should be almost instantaneous but allow it a minute for it to be delivered and create a customer profile.

8. Open the Amazon Connect agent application. Search for the user ID you entered in the **Event Builder**. You should be able to see the customer profile with the user ID and the traits you entered.

9. If you cannot see the customer profile, then there is a problem with your integration. To troubleshoot:

   1. Go to the Amazon EventBridge console.
   2. Check whether the EventSource is Active and the matching EventBus exists and is running.

   If these are working, contact AWS Support for assistance investigating the issue.
Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose Flow details to learn more about what's gone wrong.

You may need to delete the configuration and re-connect to the external application.

Set up integration for Shopify

To provide periodic updates to Amazon Connect Customer Profiles, you can integrate with Shopify using Amazon AppIntegrations. You first set up the connection in Amazon Connect and Shopify, and then verify the Shopify integration.

Set up the connection in Amazon Connect and Shopify

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

   ![Amazon Connect virtual contact center instances](image)

   - Instance alias: mytest67
   - Access URL: https://mytest67.my.connect.aws
   - Inbound, outbound telephony
   - Create date: 1/12/2022
   - Status: Active

3. In the navigation pane, choose Customer profiles.
5. **On the Select source page,** choose **Shopify.** Review the application requirements that are listed on the Select application page.

6. **On the Establish connection page,** choose one of the following:
   - **Use existing connection:** This allows you to reuse existing Amazon EventBridge resources that you may have created in your AWS account.
   - **Create new connection:** Enter the information required by the external application.
• **Connection name**: Provide a name for your connection. The connection name is referenced by integrations that use this connection.

• **Connection URL**: Enter your application connection URL. This URL is used for deep-linking into the objects created in your external application. The connection URL is the Shopify Partner app URL available on the application website.

To find your Shopify Partner app URL:

- Log in to your partners.shopify.com account.
- Go to your app.
- Copy the URL from your browser.

• **Client ID**: Enter your application client ID. This is a string that uniquely distinguishes the client in your external application. This client ID is the Source Name available on the application website. You use the ID that you specify here to identify the client that you want Customer Profiles to ingest your objects from. Your client ID may be available after following the Source setup steps.
To find your source name:

- Log in to your partners.shopify.com account.
- Go to your app.
- Copy the source name from your Amazon EventBridge event source.

7. On the Source set up page, copy your AWS account ID to your clipboard, and then choose Log in to Shopify.

8. Use the following instructions to set up Shopify:

   b. Under Amazon EventBridge, choose Create source.
   c. Paste in your AWS account ID and select your AWS Region.
   d. After you set up the event source destination, return to Customer Profiles. You will see an alert that indicates Amazon Connect has successfully connected with Shopify.

9. On the Integration options page, choose which source objects you want to ingest and select their object type.

   Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to the standard objects in Customer Profiles. You can also use the object mappings that you've created from the PutProfileObjectType.
10. For the **Ingestion start date**, Customer Profiles starts ingesting records created after the integration is added.

   ![Object type Info](image)

   **Note**

   If you need historical records, you can [use Amazon S3 as an integration source to import them](#).

11. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Add integration**.

   **Note**

   After adding this integration, you need to [set up webhook subscriptions](#) to allow events to start flowing into this integration.
12. After the integration is set up, back on the Customer profiles configuration page, the Integrations section displays which integrations are currently set up. The Last run and Integration health are not currently available for this type of integration.
To see what data is being sent, choose the integration and then choose View objects.

13. Go to the next step to use the API to set up **webhook subscriptions** so events can start flowing into this integration.

**Set up webhook subscriptions**

1. Use the following URL to make sure your app has the required permissions:

   ```
   https://{shop}.myshopify.com/admin/oauth/authorize?
   client_id={api_key}&scope={scopes}&redirect_uri={redirect_uri}&state={nonce}
   ```

   Where:

   - **shop** is the name of your Shopify store.
   - **api_key** is the API Key of your Shopify app. You can find this on the Shopify App details page.
• scopes should have the value `read_customers, read_orders, read_draft_orders`.

• `redirect_uri` is the redirect URI you specified for your app when you created it. For our purposes it can be any valid URL.

• `nonce` can be any unique value to identify a given authorization request from others. We recommend using a timestamp.

After you have constructed the URL, paste it into your browser. An installation/authorization page similar to the following image is displayed, asking the store owner to give permissions for the defined scope.

2. Choose **Install unlisted app** to install and authorize the app on behalf of your store.

You will be taken to the redirect URI that you entered with an authorization code appended to redirect URI as a query parameter. For example:

```plaintext
https://example.org/some/redirect/uri?
code={authorization_code}&hmac=da9d83c171400a41f8db91a950508985&host={base64_encoded_hostname}&timestamp=1409617544&state={nonce}&shop={shop_origin}&host={host}
```

3. Copy the `authorization_code` from this URI. You're going to use it to get a permanent access token in the next steps.

4. Go to whatever tool you use to make API calls. For example, **CURL** or **POSTMAN**.

5. To get a permanent access token, make a POST request to the Shopify Admin API to this endpoint:
with the following request body:

```
{
  "code": "authorization_code_received_from_redirect_uri",
  "client_id": "your_app_api_key",
  "client_secret": "your_app_api_secret"
}
```

This request returns the following response:

```
{
  "access_token": "permanent_access_token",
  "scope": "read_customers,read_orders,read_draft_orders"
}
```

6. Note the access_token. This is a permanent token that has the provided scope from a previous step. Now you are ready to create webhook subscriptions.

7. For the following API calls, make sure you set the HTTP header key `X-Shopify-Access-Token` to the access_token you received from the earlier call's response.

8. To setup webhook subscriptions, make the following POST request for each of the topic values listed in the next step:

   Endpoint: https://{shop}.myshopify.com/admin/api/2021-04/webhooks.json

   Request Body:

   ```
   {
     "webhook": {
       "topic": "replace_this_with_one_of_the_topics_in_the_list_below",
       "address": "this_is_the_event_source_arn_generated_when_you_created_the_event_integration",
       "format": "json"
     }
   }
   ```

9. For each subscription replace the value for topic with the following values:
You're now all set to receive events from your Shopify store. Next, verify your Shopify integration.

**Verify your Shopify integration**

1. Sign in as Admin to your Shopify Store.
2. In the left navigation menu, choose **Customers**.
3. Select **Add Customer**.
4. Enter your customer details. Be sure to enter a phone number and email. These don't have to belong to a real customer. You will delete this customer entry after verifying the integration.
5. Save the customer object.
6. The event delivery should be almost instantaneous but allow a minute for it to be delivered and to create a customer profile.
7. Open the Amazon Connect agent experience and look up the user by the email or phone number you entered into the Shopify Store. You should be able to see the customer profile with the same email or phone number.
8. If you cannot see the customer profile, then there is a problem with your integration. To troubleshoot:
   1. Go to the Amazon EventBridge console.
   2. Check whether the EventSource is Active and the matching EventBus exists and is running.
Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose Flow details to learn more about what's gone wrong.

You may need to delete the configuration and re-connect to the external application.

Set up integration for external applications using Amazon AppFlow

These integrations use Amazon AppFlow to provide periodic updates to Amazon Connect Customer Profiles. The below steps provide guidance on configuring a connector of your choosing using Amazon AppFlow, configure data mappings, and configure integrations to ingest your customer data.

For more information on Amazon AppFlow pricing, see Amazon AppFlow pricing.

For more information on Amazon AppFlow supported connectors see Supported source and destination applications.

Before you begin

When you enable Amazon Connect Customer Profiles you create a Customer Profiles domain, which is a container for all data, such as customer profiles, object types, profile keys, and encryption keys. The following are guidelines for creating Customer Profile domains:

- Each Amazon Connect instance can only be associated with one domain.
- You can create multiple domains, but they don't share external application integrations or customer data between each other.
- All the external application integrations you create are at a domain level. All of the Amazon Connect instances associated with a domain inherit the domain's integrations.

Prerequisite: Enable Customer profiles in your Amazon Connect instance
1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose Customer profiles.

4. Choose enable Customer Profiles

In the form, you will be required to complete all the mandatory fields to create a Customer Profiles domain by following the steps below:

1. **Domain Setup.** You can Create New Domain and provide a name.

2. **Encryption.** Under Specify KMS key, you can enable encryption by either selecting an existing AWS KMS key, creating a new AWS KMS key, or you can choose Select existing domain.

3. **Error Reporting.** You can provide a Dead letter queue, which is an SQS queue to handle customer profile errors

4. Choose Submit and Customer Profiles will be get created using the Contact History information of your instance.

**Set up an external application using Amazon AppFlow**

You can add an external application integration to an Amazon Connect Customer Profiles domain by using Amazon AppFlow by following steps below. You must create a flow for your data source in the Amazon AppFlow console and set Amazon Connect Customer Profiles as the destination prior to continuing in the Customer Profiles console. If you created a flow more than 14 days ago, it has expired and you will need to create a new flow for your integration.

You can optionally perform data transformations such as Arithmetic, Filter, Map, Map_all, Mask, Merge, Truncate, and Validate when using the AWS CloudFormation AWS::AppFlow::Flow Task resource prior to ingestion.

1. Log into your AWS Management Console, select Amazon AppFlow, and choose Create flow.
2. Enter the flow name and an optional flow description.

**Flow details**

**Flow name**

*Enter the flow name*

**Flow description** - *optional*

Describe the flow in your own words

*Enter flow description here*

3. You can leave the **Data encryption** section as it is since your Amazon Connect Customer Profiles domain already has an existing AWS KMS key that will be used for this Flow. You can optionally create tags and then choose **Next**.

**Data encryption**

Amazon AppFlow encrypts your access tokens, secret keys, and data in transit and data at rest. Encryption for data at rest is currently available for Amazon S3 only.

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

- [ ] Customize encryption settings (advanced)
4. Select an external application of your choice in the **Source name** dropdown and then select the next relevant field. For example, if you wish to configure Slack, select Slack from the **Source name** dropdown. You can then either select an existing Slack flow or create a new connection.

5. If you chose to create a new connection, you can then enter the external application's details such as user name, password and subdomain. You can also select the AWS KMS key for data encryption and enter the connection name to identify this connection.
6. If you choose to use an existing connection you can select the specific external application object from dropdown. For example, if choosing an existing Slack connection, you can select Conversations as the object and then choose the specific Slack channel that will be used.
7. In the **Destination details** section, select Amazon Connect as the Destination name in the dropdown and select the Customer profile domain created in the previous prerequisite step.

8. Select a flow trigger by choosing **Run on demand** or **Run flow on schedule**. Choose **Next**.

   - **Run on demand** runs the flow only when you trigger it.
   - **Run flow on schedule** runs the flow at a specific time by using a schedule. The schedule frequency is limited to 5 minutes, 15 minutes, or 1 hour.

9. Choose **Manually map fields** under **Mapping method**. Choose the source fields from external application and then choose **Map fields directly**.
10. Review and choose **Create flow**.

For more information on creating flows in the Amazon AppFlow console, see [Creating flows in Amazon AppFlow](#).

For more information on the setup of external application and many other supported applications in Amazon AppFlow, see [Supported Amazon AppFlow source and destination applications](#).

**Set up data mappings to define how external application data is mapped to a Customer Profile**

Once Amazon AppFlow integration has been set up, you need to set up data mappings in Customer Profiles to define how data from the external application will be mapped to the Customer Profile. This will allow you to customize the data that you want to use to build your unified customer profile. Choose your mapping carefully, as you will not be able to choose a different mapping after creating the integration.

For more detailed information on data mappings, see [Object type mapping](#).
1. Log into your AWS Management Console, select **Amazon Connect** and choose Customer Profiles under your connect instance alias.

2. Choose **Data mappings** and then choose **Create data mapping**. Provide a Data Mapping name and a description.
3. Under **Mapping options**, you can choose your **Data source** as the external application, the **Flow name** that you created in the previous section, and the **Data definition method** as **Mapping destination**. Under **Mapping destination** you can choose the types of customer data that wish to define for your unified customer profiles. Choose **Next**.
4. Add customer, product, case and order attributes with source, destination, and content type, then choose Next.
5. **Under Specify identifiers**, you can select various attributes from your data source object that helps distinguish your data from other data source objects. You can select attributes from unique, customer, product, case and order identifiers. For more information about identifiers, see [Standard identifiers](#).

6. Review and choose **Create Data Mapping**. The Data Mapping status will show as **Active**.
Set up integrations to ingest your customer data from an external application

Once the data mapping set up is done for an external application, you will set up the Data source integration to ingest your customer data.

1. Log into your AWS Management Console, select Amazon Connect and choose Customer Profiles under your connect instance alias.

2. Under the Data source integrations section choose Add data source integration.

3. Under the Data source dropdown, select the external application and choose Next. You also have the option to choose Create new flow which will open the Amazon AppFlow console in a new tab.
4. Under the **Flow name** dropdown, select the flow you want to use from your data source and choose **Next**.

5. Under the **Data Mapping** dropdown, select the external application data mapping for the object to define how your data source is mapped to profiles. Choose **Next**.
6. **Review and choose** Add data Source Integration. The datasource integration of the external application will initially show as pending before moving to an active state.
View the unified customer profile in Amazon Connect Customer Profile Agent CCP

Your agents will now be able to view customer data that has been imported from an external application by logging in to the Amazon Connect Agent CCP. For more information on connecting to the Amazon Connect Agent CCP, see Agent application: Everything in one place.

Your agent will need to have the appropriate security profile permissions in order to view Customer Profiles and will be able to perform searches using a key name and value in the profiles search bar.

For more information on security profile permissions, see Security profiles.

Advanced users that wish to build their own custom agent application and embedded customer profiles can use StreamsJS which will provide more customization over the agent application.

Delete/stop Customer Profiles integrations

Note

Deleting mappings will only delete objects and data associated with that specific mapping. If there are multiple objects associated with a profile, then deleting a specific mapping may not clear the profile data. If you want to delete specific data, then you would delete the mapping, but your profiles may still exist if they contain data from other mappings. This could result in additional charges for the existing profiles. You can delete a domain and all data from Customer Profiles, including all profiles, by using the Amazon Connect console or the DeleteDomain API.

Console method

- If at any time you want to stop the ingestion of customer profile data, choose the integration/mapping and then choose Delete.
- To delete the integrations, customer profiles, and all the customer profile data, you can delete your customer profiles domain in the Amazon Connect console. For more information, see Delete Customer Profiles domain.

API method

- To delete customer profiles data for a specific integration, use the DeleteProfileObjectType API.
To delete the integrations, customer profiles, and all the customer profile data, use the DeleteDomain API.

To re-enable the ingestion of customer profile data, go through the setup steps again.

Object type mapping

Contents

- Concepts and terminology for customer object type mappings
- Create an object type mapping
- Object type mapping definition details
- Additional properties of object types
- Inferred profiles
- Contact record templates
- Automatically associate the Contact Record with one profile found using the _phone key
- Examples of object type mappings
- Implicit profile object types
- Generative AI powered data mapping

Concepts and terminology for customer object type mappings

The following terminology and concepts are central to your understanding of custom object type mappings.

Standard profile object

A standard profile object is a predefined object that all profiles contain.

A standard profile object contains standard fields, such as phone numbers, email addresses, name and other standard data. This data can be retrieved in a standard format regardless of the source (for example, Salesforce, ServiceNow, or Marketo).

Profile object

A profile object is a single unit of information known about a profile. For example, the information about a phone call, a ticket, a case, or even a click-stream record from a web site.
A single profile object can be up to 250 KB and can be any structured JSON document.

- Every profile object has a type. For example, the profile object can be an Amazon Connect contact record, ServiceNow Users, or Marketo Leads.
- The type refers to the object type mapping.
- The object type mapping defines how that specific object should be ingested into Customer Profiles.

**Profile**

A *profile* contains all the information known about a specific customer or contact. It includes a single standard profile object and any number of additional profile objects.

**Object type mapping**

The *object type mapping* tells Customer Profiles how to ingest a specific type of data. It provides Customer Profiles with the following information:

- How data should be populated from the object and ingested into the standard profile object.
- What fields should be indexed in the object and how those fields should then be used to assign objects of this type to a specific profile.

**Mapping template**

A *mapping template* is a predefined object type mapping included with the Customer Profiles service.

Customer Profiles includes mapping templates for Amazon Connect contact records, Salesforce Accounts, ServiceNow Users, and Marketo Leads. For a complete list of available mapping templates, use the [ListProfileObjectTypeTemplates](#) API.

With mapping templates you can quickly ingest data from well known sources without having to specify any additional information.

**Create an object type mapping**

An object type mapping tells Customer Profiles how to ingest a specific type of data from a source application—such as Salesforce, Zendesk, or S3—into a unified standard profile object. You can then display data in that object (for example, customer address and email) to your agents using the [Amazon Connect agent application](#).

The object type mapping provides Customer Profiles with the following information:
• How data should be populated from the object and ingested into the standard profile object.
• What fields should be indexed in the object and how those fields should then be used to assign objects of this type to a specific profile.

There are two ways you can create an object type mapping:

• Use the Amazon Connect console. The user interface makes data mapping features readily accessible. For example, you can add custom attributes, and define search and unique identifiers for contact models. No coding required!
• Use the Customer Profiles API. For more information, see the Amazon Connect Customer Profiles API Reference.

This topic explains how to create a mapping using the Amazon Connect console.

Create a data mapping using the Amazon Connect console

Amazon Connect provides a no-code experience for mapping customer data from homegrown and third-party applications with Amazon S3, Salesforce, ServiceNow, Zendesk, and Marketo.

To create a data mapping, you define an object type mapping that describes what the custom profile object looks like. This mapping defines how fields from your data can be used to either populate fields in the standard profile or how they can be used to assign the data to a specific profile.

Step 1: Set up data mapping

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. In the navigation pane, choose **Customer profiles, Data mappings**.

4. Choose **Create data mapping** to get started.

5. At the **Set up data mapping** page, in the **Description** section, add a name that will help you identify the source or purpose of this mapping. This is the meta-data of the object type.

6. In the **Data source** section:
   
   a. Choose where the data is coming from, such as Salesforce or Zendesk. Based on your selection, Amazon Connect automatically selects the available destinations based on the predefined template.
   
   b. Choose the source object. This is used for you to build your unified profile.
   
   c. In the **Mapping destination** section, choose the data that you want to use to build your unified customer profile. This information can be surfaced to your flows and agents to personalize the interactions with contacts.

   For more information about supported mapping destinations, see [About mapping destinations](#).

   d. In the **Additional options** section, you can choose when to opt out of creating new profiles, and how long to retain them. These options help you manage costs.

   **Note**
   
   By default the domain retention period is 366 days. To change the retention period set on your domain, use the [UpdateDomain](#) API.

7. If you chose a source other than S3, in the **Establish a connection with application** section, choose an existing Amazon AppFlow or Amazon EventBridge connection to connect your data,
or create a new connection. You can create a new connection by entering details about your account for this data source.

After the connection is established, you will choose the objects that you want to ingest from your data source.

8. Choose Next.

Step 2: Map attributes

On the Map type attributes page, you'll see the field mappings table filled with the predefined template, based on the mapping destination. For example, it's filled with customer, product, case, or order attributes. You can change the predefined template by choosing an attribute (such as AccountNumber) and then selecting a different destination, or enter one of your own custom attributes.

The following image shows an example of the page filled with customer attributes from the template.

You can remove what you don’t want populated in the customer profile, change the source, and add custom attributes.

This mapping uses your data source to populate customer contact information, such as a phone number in the customer profile. It uses attributes from the standard profile template.
Tip

- If you choose to add custom attributes, the destination will always have the prefix `Attributes` added to it. This enables Amazon Connect to recognize that it is a custom attribute.

- Agents can now view custom attributes in the Connect Agent Application under the **Additional Information** tab sorted in alphabetical order. You can create the name of your choice for each attribute that will be displayed to agents by using the following format: `/^Attributes\.[a-zA-Z0-9]+(?:[ _-]+[a-zA-Z0-9]+)*$/`

- All ingested custom attributes will be displayed in the Connect Agent Application. If you do not wish to show certain information to your agents, do not ingest custom attributes at this time.

### Step 3: Specify identifiers

On the **Specify identifiers** page, complete the following sections. Depending on what data you're mapping, it's possible not all of these will appear on your page.
Note
The names _profileId, _orderId, _caseId, and _assetId are reserved for internal use. If you decide to use these names as one of your identifier names, they must be declared as LOOKUP_ONLY, which means our system will not save them to match with profiles, standard assets, standard orders, standard cases, or save them for searching your profile, asset, case, or order. If you would like these keys to be usable for searching and matching, you must rename your key. For more information on the LOOKUP_ONLY standard identifier, see Standard identifiers.

- **Unique identifier**: You must have a unique identifier for your data in order to avoid an error when it is ingested. This identifier is also known as the unique key. Customer Profiles uses it to distinguish this data from other data source objects, and to index for search and update data.

  There can be only one unique identifier.

- **Customer identifier**: You must have at least one customer identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the profile key.

  Customer Profiles uses it to determine if the data case be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have multiple customer identifiers.

Tip
Agents can use any of these customer Identifiers in the Agent Workspace to find the profile that belongs to customer on the interaction.

- **Product identifier**: You must have at least one product identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the asset key.

  Customer Profiles uses it to distinguish this data from other customer product purchase data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have multiple product identifiers.
• **Case identifier**: You must have at least one case identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the case key.

Customer Profiles uses it to distinguish this data from other customer case data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

You can have multiple case identifiers.

• **Order identifier**: You must have at least one order identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the order key.

Customer Profiles uses it to distinguish this data from other customer order data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

You can have multiple order identifiers.

• **Additional search attributes - optional**: You can choose attributes in your data source object that you want to index to be searchable. By default, all your identifiers are indexed.

• **Data object timestamp**: The data object timestamp is used to resolve profile conflicts when Identity Resolution is enabled for consolidating similar profiles. When two or more similar profiles have conflicting records, the records from the profile with the most recently updated timestamp will be used.

You can choose an attribute in your object to reference for when your object was last updated.

**Step 4: Review and create**

After the data mapping is created, you can choose **Add data source integration** to use this object type.
About mapping destinations

A mapping destination is your mapping from a source to a standard definition that is already defined in Amazon Connect.

The following table lists the supported mapping destinations.

<table>
<thead>
<tr>
<th>Source object</th>
<th>Destination: Customer, Product, Order, Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3</td>
<td>Any</td>
</tr>
<tr>
<td>Salesforce-Account</td>
<td>Customer</td>
</tr>
<tr>
<td>Salesforce-Contact</td>
<td>Customer</td>
</tr>
<tr>
<td>Salesforce-Asset</td>
<td>Product</td>
</tr>
<tr>
<td>Zendesk-users</td>
<td>Customer</td>
</tr>
<tr>
<td>Marketo-leads</td>
<td>Customer</td>
</tr>
<tr>
<td>Servicenow-sys_user</td>
<td>Customer</td>
</tr>
</tbody>
</table>
Object type mapping requirements

The following information needs to be in your object type mapping so Customer Profiles can process the incoming data:

- A definition of all the fields in the ingested object that should be mapped to the standard profile, or used for assigning the data to a profile. This tells Customer Profiles which fields in the ingested source object should be mapped to given fields in the standard profile object.
- Which fields in the source object from your custom data should be indexed and how.

When the source data is ingested by Customer Profiles, the indexed fields determine:

- Which profile a specific object belongs to.
- Which objects are related to each other and should be placed in the same profile. For example, an account number or a contact ID in a contact record.
- What values can be used to find a profile. For example, the contact's name can be indexed. This would allow agents to find all profiles that belong to customers with a specific name.

Key requirements

You must define at least one key. Customer Profiles uses this key to map your custom profile object to a profile.
The custom profile object mapping also needs at least one key that uniquely identifies the object so that it can be updated by specifying the same value of this field (these requirements can be satisfied with a single key).

Each key can be made up of one or more fields.

**Field requirements**

A field definition specifies how to read a value for that field name from a source object. The field definition also specifies what kind of data is stored in the field.

Object type names can be any alpha numerical string or the '-' and '_' character, they also cannot start with a '_' character, which is used for reserved standard object types.

**Object type mapping definition details**

The object type mapping definition has two parts: the field definition and the key definition.

---

**Tip**

To learn how to create an object type mapper, see this blog post: [Unify and organize customer information with Amazon Connect Customer Profiles with the pre-built Amazon S3 connector](https://yourblogpost.com). Or, check out this video on YouTube: [How to Integrate Customer Profile Data into your Contact Center Experiences](https://yourvideolink.com).

---

**Field definition details**

The field definition defines the source, destination (target), and type of field. For example:

```
"Fields": {
    "{fieldName}": {
        "Source": "{source}",
        "Target": "{target}",
        "ContentType": "{contentType}"
    }, ...
}, ...
```

- **Source**: This can be a JSON accessor for the field or a Handlebar macro for generating the value of the field.
The source object being parsed is named `_source` so all fields in the source fields need to be prefaced by this string. Only the `_source` object is supported.

Use the Handlebar macro solution for generating constants and combining multiple source object fields into a single field. This is useful for indexing.

- **Target**: Specifies where in a standard object type the data of this field should be mapped.

  Populating the standard profile allows you to use data ingested from any data source with applications built on top of Customer Profiles without any specific knowledge of the format of the data being ingested.

  This field is optional. You might want to define fields solely for the purpose of including them in a key.

  The format of this field is always a JSON accessor. The only supported target object is `_profile`.

- **ContentType**: The following values are supported STRING, NUMBER, PHONE_NUMBER, EMAIL_ADDRESS, NAME. If no `ContentType` is specified STRING is assumed.

  `ContentType` is used to determine how to index the value so agents can search for it. For example, if `ContentType` is set to PHONE_NUMBER, a phone number is processed so agents can search for it in any format: the string "+15551234567" matches "+(555)-123-4567".

**Key definition details**

A key contains one or more fields that together define a key that can be used to search for objects (or the profiles they belong to) using the SearchProfiles API. The key can also be defined to uniquely identify a profile or uniquely identify the object itself.

```json
"Keys": {
    "{keyName}": [
        {
            "StandardIdentifiers": [...],
            "FieldNames": [ "{fieldname}", ... ]
        }, ...
    ], ...
}
```

Key names are global to a domain. If you have two keys, with the same name in two different object type mappings:
• Those keys should occupy the same namespace
• They can be used to potentially link profiles together between different objects. If they match between the objects, Customer Profiles places the two objects in the same profile.

To phrase this in another way: keys should have the same key name in a domain if, and only if, the same value means that they are related. For example, a phone number specified in one type of object would be related to the same phone number specified in another type of object. An internal identifier specified for an imported object from Salesforce might not be related to another object imported from Marketo, even if they have exactly the same value.

Keys definitions are used in two ways:

• Inside of Customer Profiles during ingestion, they are used to figure out what profile the object should be assigned to.
• They allow you to use the SearchProfiles API to search for the key value and find the profile.

### Standard identifiers

Standard identifiers allow you to set attributes on the key. Decide which identifiers to use based on how you want the data to be ingested in the profiles. For example, you mark phone number with the identifier PROFILE. This means phone number is to be treated as unique identifier. If Customer Profiles gets two contacts with the same phone number, the contacts are going to be merged into a single profile.

<table>
<thead>
<tr>
<th>Identifier name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIQUE</td>
<td></td>
</tr>
</tbody>
</table>

This identifier must be specified by exactly one index for each object type. This key is used to uniquely identify objects of the object type for either fetching them or if needed update a submitted object at a later date.

All the fields that make up the UNIQUE keys are required to be specified when submitting a new object or it is rejected.
<table>
<thead>
<tr>
<th>Identifier name</th>
<th>Description</th>
</tr>
</thead>
</table>
| PROFILE         | This identifier means that this key uniquely identifies a profile. When this identifier is specified, it means that during ingestion, Customer Profiles looks for any profile that has this key associated with it.  
- If a profile is found, then the object is assigned to that profile.  
- If more than one profile is found when searching for this key, the match is rejected. (Only keys that uniquely identify a profile should be used as unique keys except for special circumstances.) |
<table>
<thead>
<tr>
<th>Identifier name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOOKUP_ONLY</td>
<td>This identifier indicates the key is not stored after ingesting the object. The key is only to be used for determining the profile during ingestion. The key value is not associated with the profile during ingestion, which means it can't be used to allow searching for it or matching later ingested objects to the same key.</td>
</tr>
</tbody>
</table>

**Note**
- You cannot specify a key as both a UNIQUE identifier and a LOOKUP_ONLY identifier.
- You can only use PROFILE together with LOOKUP_ONLY if there is at least one other key that has the PROFILE identifier without the NEW_ONLY or LOOKUP_ONLY identifiers.
<table>
<thead>
<tr>
<th>Identifier name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW_ONLY</td>
<td>If the profile does not already exist before the object is ingested, the key is associated with the profile. Otherwise the key is only used for matching objects to profiles.</td>
</tr>
</tbody>
</table>

**Note**
- You cannot specify a key as both a UNIQUE identifier and a NEW_ONLY identifier.
- You can only use PROFILE together with NEW_ONLY if there is at least one other key that has the PROFILE identifier without the NEW_ONLY or LOOKUP_ONLY identifiers.

| SECONDARY       | During the matching of an object to a profile, Customer Profiles first looks up all PROFILE keys that do not have the SECONDARY identifier. These are considered first. SECONDARY keys are only considered if no matching profile is found using these keys. |
### Identifier name | Description
--- | ---
**ASSET** | This identifier means that this key uniquely identifies an asset. When this identifier is specified, it means that during ingestion, Customer Profiles looks for any asset that has this key associated with it.  
- If an asset is found, then the object is assigned to that asset.  
- If more than one asset is found when searching for this key, the match is rejected. (Only keys that uniquely identify an asset should be used as unique keys except for special circumstances.)

**ORDER** | This identifier means that this key uniquely identifies an order. When this identifier is specified, it means that during ingestion, Customer Profiles looks for any order that has this key associated with it.  
- If an order is found, then the object is assigned to that order.  
- If more than one order is found when searching for this key, the match is rejected. (Only keys that uniquely identify an order should be used as unique keys except for special circumstances.)
<table>
<thead>
<tr>
<th>Identifier name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASE</td>
<td>This identifier means that this key uniquely identifies a case. When this identifier is specified, it means that during ingestion, Customer Profiles looks for any case that has this key associated with it.</td>
</tr>
<tr>
<td></td>
<td>• If a case is found, then the object is assigned to that case.</td>
</tr>
<tr>
<td></td>
<td>• If more than one case is found when searching for this key, the match is rejected. (Only keys that uniquely identify a case should be used as unique keys except for special circumstances.)</td>
</tr>
</tbody>
</table>

**How profile assignment works using key definitions**

When Customer Profiles ingests the custom object mappings, it processes the key definitions. The following diagram shows how it processes standard identifiers in key definitions to determine which profile to assign the object to.
How keys are added to the index for future lookups

The following diagram shows how Customer Profiles processes the standard identifiers to determine whether to persist the key.
Object type mapping for the standard profile

The topics in this section provide the standard profile definition, and the object type mapping from external applications to the standard profile.

Contents

- Amazon AppFlow access requirements
- Amazon AppIntegrations access requirements
- **Amazon EventBridge access requirements**
- **Standard profile definition**
- **Mapping Salesforce objects to the standard profile**
- **Mapping Zendesk objects to the standard profile**
- **Mapping Marketo objects to the standard profile**
- **Mapping ServiceNow objects to the standard profile object**
- **Mapping Segment objects to the standard profile object**
- **Mapping Shopify objects to the standard profile object**

**Amazon AppFlow access requirements**

Following are the Amazon AppFlow access requirements to create and delete Zendesk, Marketo, Salesforce, and ServiceNow integrations:

- `appflow:CreateFlow`
- `appflow:DeleteFlow`

**Amazon AppIntegrations access requirements**

Following are the Amazon AppIntegrations access requirements to create and delete Segment and Shopify integrations:

- `app-integrations:GetEventIntegration`
- `app-integrations:ListEventIntegrationAssociations`
- `app-integrations:CreateEventIntegrationAssociation`
- `app-integrations:DeleteEventIntegrationAssociation`

**Amazon EventBridge access requirements**

Following are the Amazon EventBridge access requirements to create and delete Segment and Shopify integrations:

- `events:ListTargetsByRule`
- `events:PutRule`
- `events:PutTargets`
- events:DeleteRule
- events:RemoveTargets

**Standard profile definition**

The following table lists all the fields in the Customer Profiles standard profile object.

<table>
<thead>
<tr>
<th>Standard profile field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProfileId</td>
<td>String</td>
<td>The unique identifier of a customer profile.</td>
</tr>
<tr>
<td>AccountNumber</td>
<td>String</td>
<td>A unique account number that you have given to the customer.</td>
</tr>
<tr>
<td>AdditionalInformation</td>
<td>String</td>
<td>Any additional information relevant to the customer's profile.</td>
</tr>
<tr>
<td>PartyType</td>
<td>String</td>
<td>The type of profile used to describe the customer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values: INDIVIDUAL</td>
</tr>
<tr>
<td>BusinessName</td>
<td>String</td>
<td>The name of the customer's business.</td>
</tr>
<tr>
<td>FirstName</td>
<td>String</td>
<td>The customer's first name.</td>
</tr>
<tr>
<td>MiddleName</td>
<td>String</td>
<td>The customer's middle name.</td>
</tr>
<tr>
<td>LastName</td>
<td>String</td>
<td>The customer's last name.</td>
</tr>
<tr>
<td>BirthDate</td>
<td>String</td>
<td>The customer's birth date.</td>
</tr>
<tr>
<td>Gender</td>
<td>String</td>
<td>The gender with which the customer identifies.</td>
</tr>
<tr>
<td>Standard profile field</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PhoneNumber</td>
<td>String</td>
<td>The customer's phone number, which has not been specified as a mobile, home, or business number.</td>
</tr>
<tr>
<td>MobilePhoneNumber</td>
<td>String</td>
<td>The customer's mobile phone number.</td>
</tr>
<tr>
<td>HomePhoneNumber</td>
<td>String</td>
<td>The customer's home phone number.</td>
</tr>
<tr>
<td>BusinessPhoneNumber</td>
<td>String</td>
<td>The customer's business phone number.</td>
</tr>
<tr>
<td>EmailAddress</td>
<td>String</td>
<td>The customer's email address, which has not been specified as a personal or business address.</td>
</tr>
<tr>
<td>BusinessEmailAddress</td>
<td>String</td>
<td>The customer's business email address.</td>
</tr>
<tr>
<td>Address</td>
<td>Address</td>
<td>A generic address associated with the customer that is not mailing, shipping, or billing.</td>
</tr>
<tr>
<td>ShippingAddress</td>
<td>Address</td>
<td>The customer's shipping address.</td>
</tr>
<tr>
<td>MailingAddress</td>
<td>Address</td>
<td>The customer's mailing address.</td>
</tr>
<tr>
<td>BillingAddress</td>
<td>Address</td>
<td>The customer's billing address.</td>
</tr>
<tr>
<td>Attributes</td>
<td>String-to-string map</td>
<td>Key-value pair of attributes of a customer profile.</td>
</tr>
</tbody>
</table>
Address data type

<table>
<thead>
<tr>
<th>Standard profile field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address1</td>
<td>String</td>
<td>The first line of a customer address.</td>
</tr>
<tr>
<td>Address2</td>
<td>String</td>
<td>The second line of a customer address.</td>
</tr>
<tr>
<td>Address3</td>
<td>String</td>
<td>The third line of a customer address.</td>
</tr>
<tr>
<td>Address4</td>
<td>String</td>
<td>The fourth line of a customer address.</td>
</tr>
<tr>
<td>City</td>
<td>String</td>
<td>The city in which the customer lives.</td>
</tr>
<tr>
<td>Country</td>
<td>String</td>
<td>The country in which the customer lives.</td>
</tr>
<tr>
<td>County</td>
<td>String</td>
<td>The county in which the customer lives.</td>
</tr>
<tr>
<td>PostalCode</td>
<td>String</td>
<td>The postal code of the customer address.</td>
</tr>
<tr>
<td>Province</td>
<td>String</td>
<td>The province in which the customer lives.</td>
</tr>
<tr>
<td>State</td>
<td>String</td>
<td>The state in which the customer lives.</td>
</tr>
</tbody>
</table>

Mapping Salesforce objects to the standard profile

This topic lists which fields in Salesforce objects map to fields in the standard profile object in Customer Profiles.
Salesforce-Account object

Following is a list of all the fields in a Salesforce-Account object. The fields in your Salesforce-Account object may vary depending on the configuration of your Salesforce instance.

- Id
- IsDeleted
- MasterRecordId
- Name
- Type
- ParentId
- BillingStreet
- BillingCity
- BillingState
- BillingPostalCode
- BillingCountry
- BillingLatitude
- BillingLongitude
- BillingGeocodeAccuracy
- BillingAddress.City
- BillingAddress.Country
- BillingAddress.geocodeAccuracy
- BillingAddress.latitude
- BillingAddress.longitude
- BillingAddress.postalCode
- BillingAddress.state
- ShippingStreet
- ShippingCity
- ShippingState
- ShippingPostalCode
- ShippingCountry
- ShippingLatitude
- ShippingLongitude
- ShippingGeocodeAccuracy
- ShippingAddress.city
- ShippingAddress.country
- ShippingAddress.latitude
- ShippingAddress.longitude
- ShippingAddress.postalCode
- ShippingAddress.state
- ShippingAddress.street
- Phone
- Fax
- AccountNumber
- Website
- PhotoUrl
- Sic
- Industry
- AnnualRevenue
- NumberOfEmployees
- Ownership
- TickerSymbol
- Description
- Rating
- Site
- OwnerId
- CreatedDate
- CreatedById
- LastModifiedDate
- LastModifiedId
- SystemModstamp
• LastActivityDate
• LastViewedDate
• LastReferencedDate
• Jigsaw
• JigsawCompanyId
• CleanStatus
• AccountSource
• DunsNumber
• Tradestyle
• NaicsCode
• NaicsDesc
• YearStarted
• SicDesc
• DandbCompanyId
• IsBuyer

**Mapping a Salesforce-Account object to a standard profile**

A subset of the fields in the Salesforce-Account object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Salesforce-Account object to the standard profile. (The table includes the mapping for a Salesforce instance that has been configured to include Person fields.)

<table>
<thead>
<tr>
<th>Salesforce-Account source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Attributes.sfdcAccountId</td>
</tr>
<tr>
<td>Name</td>
<td>BusinessName</td>
</tr>
<tr>
<td>Phone</td>
<td>PhoneNumber</td>
</tr>
<tr>
<td>BillingStreet</td>
<td>BillingAddress.Address1</td>
</tr>
<tr>
<td>Salesforce-Account source field</td>
<td>Standard profile target field</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>BillingCity</td>
<td>BillingAddress.City</td>
</tr>
<tr>
<td>BillingState</td>
<td>BillingAddress.State</td>
</tr>
<tr>
<td>ShippingStreet</td>
<td>ShippingAddress.Address1</td>
</tr>
<tr>
<td>ShippingCity</td>
<td>ShippingAddress.City</td>
</tr>
<tr>
<td>ShippingState</td>
<td>ShippingAddress.State</td>
</tr>
<tr>
<td>ShippingCountry</td>
<td>ShippingAddress.Country</td>
</tr>
<tr>
<td>ShippingPostalCode</td>
<td>ShippingAddress.PostalCode</td>
</tr>
<tr>
<td>IsPersonAccount</td>
<td>PartyType</td>
</tr>
<tr>
<td>PersonMobilePhone</td>
<td>MobilePhoneNumber</td>
</tr>
<tr>
<td>PersonHomePhone</td>
<td>HomePhoneNumber</td>
</tr>
<tr>
<td>PersonEmail</td>
<td>PersonalEmailAddress</td>
</tr>
<tr>
<td>PersonMailingAddress.Street</td>
<td>MailingAddress.Address1</td>
</tr>
<tr>
<td>PersonMailingAddress.City</td>
<td>MailingAddress.City</td>
</tr>
<tr>
<td>PersonMailingAddress.State</td>
<td>MailingAddress.State</td>
</tr>
<tr>
<td>PersonMailingAddress.Country</td>
<td>MailingAddress.Country</td>
</tr>
<tr>
<td>PersonMailingAddress.PostalCode</td>
<td>MailingAddress.PostalCode</td>
</tr>
<tr>
<td>PersonBirthDate</td>
<td>BirthDate</td>
</tr>
<tr>
<td>PersonOtherStreet</td>
<td>Address.Address1</td>
</tr>
</tbody>
</table>
The Salesforce-Account customer data from the Salesforce object is associated with an Amazon Connect customer profile using the indexes in the following table.

<table>
<thead>
<tr>
<th><strong>Salesforce-Account source field</strong></th>
<th><strong>Standard profile target field</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>PersonOtherCity</td>
<td>Address.City</td>
</tr>
<tr>
<td>PersonOtherState</td>
<td>Address.State</td>
</tr>
<tr>
<td>PersonOtherCountry</td>
<td>Address.Country</td>
</tr>
<tr>
<td>PersonOtherPostalCode</td>
<td>Address.PostalCode</td>
</tr>
<tr>
<td>FirstName</td>
<td>FirstName</td>
</tr>
<tr>
<td>LastName</td>
<td>LastName</td>
</tr>
<tr>
<td>MiddleName</td>
<td>MiddleName</td>
</tr>
<tr>
<td>AccountNumber</td>
<td>AccountNumber</td>
</tr>
</tbody>
</table>

For example, you can use _salesforceAccountId as a key name with the SearchProfiles API to find a profile. You can find the Salesforce-Account objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectType Name set to Salesforce-Account.

**Salesforce-Contact object**

Following is a list of all the fields in a Salesforce-Contact object.

- Id
- IsDeleted
- MasterRecordId
- AccountId
• LastName
• FirstName
• Salutation
• Name
• OtherStreet
• OtherCity
• OtherState
• OtherPostalCode
• OtherCountry
• OtherLatitude
• OtherLongitude
• OtherGeocodeAccuracy
• OtherAddress.city
• OtherAddress.country
• OtherAddress.geocodeAccuracy
• OtherAddress.latitude
• OtherAddress.postalCode
• OtherAddress.state
• OtherAddress.street
• MailingStreet
• MailingCity
• MailingState
• MailingPostalCode
• MailingCountry
• MailingLatitude
• MailingLongitude
• MailingGeocodeAccuracy
• MailingAddress.city
- MailingAddress.country
- MailingAddress.geocodeAccuracy
- MailingAddress.latitude
- MailingAddress.longitude
- MailingAddress.postalCode
- MailingAddress.state
- MailingAddress.street
- Phone
- Fax
- MobilePhone
- HomePhone
- OtherPhone
- AssistantPhone
- ReportsTold
- Email
- Title
- Department
- AssistantName
- LeadSource
- Birthdate
- Description
- OwnerId
- CreatedDate
- CreatedById
- LastModifiedByld
- LastModifiedDate
- LastModifiedById
- SystemModstamp
- LastActivityDate
Mapping a Salesforce-Contact object to a standard profile

A subset of the fields in the Salesforce-Contact object map to the standard profile object in Customer Profiles. The following table lists which fields can be mapped from the Salesforce-Contact object to the standard profile object.

<table>
<thead>
<tr>
<th>Salesforce-Contact source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Attributes.sfdcContactId</td>
</tr>
<tr>
<td>AccountId</td>
<td>Attributes.sfdcAccountId</td>
</tr>
<tr>
<td>LastName</td>
<td>LastName</td>
</tr>
<tr>
<td>FirstName</td>
<td>FirstName</td>
</tr>
<tr>
<td>MiddleName</td>
<td>MiddleName</td>
</tr>
<tr>
<td>OtherStreet</td>
<td>Address.Address1</td>
</tr>
<tr>
<td>OtherCity</td>
<td>Address.City</td>
</tr>
<tr>
<td>OtherState</td>
<td>Address.State</td>
</tr>
<tr>
<td>Salesforce-Contact source field</td>
<td>Standard profile target field</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>OtherCountry</td>
<td>Address.Country</td>
</tr>
<tr>
<td>OtherPostalCode</td>
<td>Address.PostalCode</td>
</tr>
<tr>
<td>MailingStreet</td>
<td>MailingAddress.Address1</td>
</tr>
<tr>
<td>MailingCity</td>
<td>MailingAddress.City</td>
</tr>
<tr>
<td>MailingState</td>
<td>MailingAddress.State</td>
</tr>
<tr>
<td>MailingCountry</td>
<td>MailingAddress.Country</td>
</tr>
<tr>
<td>MailingPostalCode</td>
<td>MailingAddress.PostalCode</td>
</tr>
<tr>
<td>Phone</td>
<td>PhoneNumber</td>
</tr>
<tr>
<td>HomePhone</td>
<td>HomePhoneNumber</td>
</tr>
<tr>
<td>MobilePhone</td>
<td>MobilePhoneNumber</td>
</tr>
<tr>
<td>Email</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>Birthdate</td>
<td>BirthDate</td>
</tr>
</tbody>
</table>

The Salesforce-Contact customer data from a Salesforce object is associated with an Amazon Connect customer profile using the indexes in the following table.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Salesforce-Contact source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_salesforceContactId</td>
<td>Id</td>
</tr>
<tr>
<td>_salesforceAccountId</td>
<td>AccountId</td>
</tr>
</tbody>
</table>

For example, you can use _salesforceAccountId and _salesforceContactId as a key name with the SearchProfiles API to find a profile. You can find the Salesforce-Contact objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectType set to Salesforce-Contact.
Mapping Zendesk objects to the standard profile

This topic lists which fields in Zendesk objects map to fields in the standard profile in Customer Profiles.

**Zendesk-users object**

Following is a list of all the fields in a Zendesk-users object.

- id
- url
- external_id
- email
- active
- chat_only
- customer_role_id
- role_type
- details
- last_login_at
- locale
- locale_id
- moderator
- notes
- only_private_comments
- default_group_id
- phone
- shared_phone_number
- photo
- restricted_agent
- role
- shared
• tags
• signature
• suspended
• ticket_restriction
• time_zone
• two_factor_auth_enabled
• user_fields
• verified
• report_csv
• created_at
• updated_at

Mapping Zendesk users to a standard profile

A subset of the fields in the Zendesk-users object map to the standard profile in Customer Profiles. The following table lists which fields can be mapped from the Zendesk-users object to the standard profile.

<table>
<thead>
<tr>
<th>Zendesk-users source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Attributes.ZendeskUserId</td>
</tr>
<tr>
<td>external_id</td>
<td>Attributes.ZendeskExternalId</td>
</tr>
<tr>
<td>email</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>phone</td>
<td>PhoneNumber</td>
</tr>
</tbody>
</table>

The Zendesk-users customer data from the Zendesk object is associated with a Amazon Connect customer profile using the following indexes.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Zendesk-user source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_zendeskUserId</td>
<td>Id</td>
</tr>
<tr>
<td>Standard Index Name</td>
<td>Zendesk-user source field</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>_zendeskExternalId</td>
<td>external_id</td>
</tr>
</tbody>
</table>

For example, you can use _zendeskUserId and _zendeskExternalId as a key name with the **SearchProfiles** API to find an Amazon Connect customer profile. You can find the Zendesk-users objects associated with a specific customer profile by using the **ListProfileObjects** API with the ProfileId and ObjectTypeNameset to Zendesk-users.

**Mapping Marketo objects to the standard profile**

This topic lists which fields in Marketo objects map to fields in the standard profile object in Customer Profiles.

**Marketo-leads object**

Following is a list of all the fields in a Marketo-leads object:

- id
- firstName
- lastName
- middleName
- email
- phone
- mobilePhone
- billingStreet
- billingCity
- billingState
- billingCountry
- billingPostalCode
- address
- city
- state
- country
• postalcode
• gender
• dateOfBirth

Mapping Marketo-leads to a standard profile

A subset of fields in the Marketo-leads object map to the standard profile.

<table>
<thead>
<tr>
<th>Marketo-leads source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Attributes.MarketoLeadId</td>
</tr>
<tr>
<td>sfdcAccountId</td>
<td>Attributes.sfdcAccountId</td>
</tr>
<tr>
<td>sfdcContactId</td>
<td>Attributes.sfdcContactId</td>
</tr>
<tr>
<td>firstName</td>
<td>FirstName</td>
</tr>
<tr>
<td>lastName</td>
<td>LastName</td>
</tr>
<tr>
<td>middleName</td>
<td>MiddleName</td>
</tr>
<tr>
<td>email</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>phone</td>
<td>PhoneNumber</td>
</tr>
<tr>
<td>mobilePhone</td>
<td>MobilePhoneNumber</td>
</tr>
<tr>
<td>billingStreet</td>
<td>BillingAddress.Address1</td>
</tr>
<tr>
<td>billingCity</td>
<td>BillingAddress.City</td>
</tr>
<tr>
<td>billingState</td>
<td>BillingAddress.State</td>
</tr>
<tr>
<td>billingCountry</td>
<td>BillingAddress.Country</td>
</tr>
<tr>
<td>billingPostalCode</td>
<td>BillingAddress.PostalCode</td>
</tr>
<tr>
<td>address</td>
<td>Address.Address1</td>
</tr>
<tr>
<td>Marketo-leads source field</td>
<td>Standard profile target field</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>city</td>
<td>Address.City</td>
</tr>
<tr>
<td>state</td>
<td>Address.State</td>
</tr>
<tr>
<td>country</td>
<td>Address.Country</td>
</tr>
<tr>
<td>postalcode</td>
<td>Address.PostalCode</td>
</tr>
<tr>
<td>gender</td>
<td>Gender</td>
</tr>
<tr>
<td>dataOfBirth</td>
<td>BirthDate</td>
</tr>
</tbody>
</table>

The Marketo-leads customer data from Marketo is associated with an Amazon Connect customer profile using the indexes in the following table.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Marketo-leads source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_marketoLeadId</td>
<td>id</td>
</tr>
<tr>
<td>_salesforceAccountId</td>
<td>sfdcAccountId</td>
</tr>
<tr>
<td>_salesforceContactId</td>
<td>sfdcContactId</td>
</tr>
</tbody>
</table>

For example, you can use _marketoLeadId, _salesforceAccountId, and _salesforceContactId as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Marketo-leads objects associated with a specific customer profile by using the ListProfileObjects API with the ProfileId and ObjectTypeName set to Marketo-leads.

### Mapping ServiceNow objects to the standard profile object

This topic lists which fields in ServiceNow objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

#### Servicenow-sys_user object

Following is a list of all the fields in a Servicenow-sys_user object
• sys_id
• active
• building
• calendar_integration
• city
• company
• cost_center
• country
• date_format
• default_perspective
• department
• edu_status
• email
• employee_number
• enable_multifactor_authn
• failed_attempts
• first_name
• gender
• home_phone
• internal_integration_user
• introduction
• last_login
• last_login_device
• last_login_time
• last_name
• last_password
• ldap_server
• location
• locked_out
• manager
• middle_name
• mobile_phone
• name
• notification
• password_needs_reset
• phone
• photo
• preferred_language
• roles
• schedule
• source
• state
• street
• sys_class_name
• sys_created_by
• sys_created_on
• sys_domain.link
• sys_domain.value
• sys_domain_path
• sys_id
• sys_mod_count
• sys_updated_by
• sys_updated_on
• time_format
• time_zone
• title
• user_name
• user_password
• web_service_access_only
• zip

Mapping Servicenow-sys_users to a standard profile object

A subset of the fields in the Servicenow-sys_users object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-sys_users object to the standard profile.

<table>
<thead>
<tr>
<th>Servicenow-sys_users source field</th>
<th>Customer profiles target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_id</td>
<td>Attributes.ServiceNowSystemId</td>
</tr>
<tr>
<td>first_name</td>
<td>FirstName</td>
</tr>
<tr>
<td>last_name</td>
<td>LastName</td>
</tr>
<tr>
<td>middle_name</td>
<td>MiddleName</td>
</tr>
<tr>
<td>gender</td>
<td>Gender</td>
</tr>
<tr>
<td>email</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>phone</td>
<td>PhoneNumber</td>
</tr>
<tr>
<td>home_phone</td>
<td>HomePhoneNumber</td>
</tr>
<tr>
<td>mobile_phone</td>
<td>MobilePhoneNumber</td>
</tr>
<tr>
<td>street</td>
<td>Address.Address1</td>
</tr>
<tr>
<td>city</td>
<td>Address.City</td>
</tr>
<tr>
<td>state</td>
<td>Address.State</td>
</tr>
<tr>
<td>country</td>
<td>Address.Country</td>
</tr>
</tbody>
</table>

Object type mapping definition details
### Servicenow-sys_users source field | Customer profiles target field
--- | ---
zip | Address.PostalCode

The Servicenow-sys_user customer data from Servicenow object is associated with an Amazon Connect customer profile using the indexes in the following table.

### Standard Index Name | Servicenow-sys_user source field
--- | ---
_serviceNowSystemId | sys_id

For example, you can use _serviceNowSystemId and _serviceNowIncidentId as a key name with the [SearchProfiles](#) API to find an Amazon Connect customer profile. You can find the Servicenow-sys_user objects associated with a specific profile by using the [ListProfileObjects](#) API with the ProfileId and ObjectType Name set to Servicenow-sys_user.

### Mapping Segment objects to the standard profile object

This topic lists which fields in Segment objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

#### Segment-Identify object

Following is a list of all the fields in a Segment-Identify object.

- userId
- common fields - see [Spec: Common Fields](#) in the Segment documentation
- Segment reserved traits - see [Traits](#) in the Segment documentation
- traits.address.street
- traits.address.city
- traits.address.state
- traits.address.postalCode
- traits.address.country
- traits.age
- traits.avatar
• traits.birthday
• traits.company.name
• traits.company.id
• traits.company.industry
• traits.company.employee_count
• traits.company.plan
• traits.createdAt
• traits.description
• traits.email
• traits.firstName
• traits.gender
• traits.id
• traits.lastName
• traits.name
• traits.phone
• traits.title
• traits.username
• traits.website

Mapping a Segment-Identify to a standard profile object

A subset of the fields in the Segment-Identify object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Segment-Identify object to the standard profile.

<table>
<thead>
<tr>
<th>Segment-Identify source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>userId</td>
<td>Attributes.SegmentUserId</td>
</tr>
<tr>
<td>traits.company.name</td>
<td>BusinessName</td>
</tr>
<tr>
<td>traits.firstName</td>
<td>FirstName</td>
</tr>
</tbody>
</table>
traits.lastName  LastName
traits.birthday  BirthDate
traits.gender  Gender
traits.phone  PhoneNumber
traits.email  EmailAddress
traits.address.street  Address.Address1
traits.address.city  Address.City
traits.address.state  Address.State
traits.address.country  Address.Country
traits.address.postalCode  Address.PostalCode

Example

The following example shows how to map a source field to a target field.

```
"segmentUserId": {
  "Source": "_source.detail.event.detail.userId",
  "Target": "_profile.Attributes.SegmentUserId"
}
```

The Segment-Identify customer data from the Segment object is associated with an Amazon Connect customer profile using the following index.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Segment-Identify source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_segmentUserId</td>
<td>userId</td>
</tr>
</tbody>
</table>

For example, you can use _segmentUserId as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Segment-Identify objects associated with a
specific profile by using the ListProfileObjects API with the ProfileId and ObjectTypeName set to Segment-Identify.

**Mapping Shopify objects to the standard profile object**

This topic lists which fields in Shopify objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

**Shopify-Customer object**

Following is a list of all the fields in a Shopify-Customer object.

- accepts_marketing
- accepts_marketing_updated_at
- addresses
- currency
- created_at
- default_address.address1
- default_address.address2
- default_address.city
- default_address.company
- default_address.country
- default_address.country_code
- default_address.country_name
- default_address.customer_id
- default_address.default
- default_address.first_name
- default_address.id
- default_address.last_name
- default_address.name
- default_address.phone
- default_address.province
- default_address.province_code
- default_address.zip
- email
- first_name
- id
- last_name
- last_order_id
- last_order_name
- metafield.key
- metafield.value
- metafield.namespace
- metafield.value_type
- marketing_opt_in_level
- multipass_identifier
- note
- orders_count
- phone
- sms_marketing_consent.state
- sms_marketing_consent.opt_in_level
- sms_marketing_consent.consent_updated_at
- sms_marketing_consent.consent_collected_from
- state
- tags
- tax_exempt
- tax_exemptions
- total_spent
- updated_at
- verified_email
Mapping a Shopify-Customer object to a standard profile

A subset of the fields in the Shopify-Customer object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-Customer object to the standard profile.

<table>
<thead>
<tr>
<th>Shopify-Customer source field</th>
<th>Standard profile target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Attributes.ShopifyCustomerId</td>
</tr>
<tr>
<td>email</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>first_name</td>
<td>FirstName</td>
</tr>
<tr>
<td>last_name</td>
<td>LastName</td>
</tr>
<tr>
<td>note</td>
<td>AdditionalInformation</td>
</tr>
<tr>
<td>phone</td>
<td>PhoneNumber</td>
</tr>
<tr>
<td>default_address.address1</td>
<td>Address.Address1</td>
</tr>
<tr>
<td>default_address.address2</td>
<td>Address.Address2</td>
</tr>
<tr>
<td>default_address.city</td>
<td>Address.City</td>
</tr>
<tr>
<td>default_address.province</td>
<td>Address.Province</td>
</tr>
<tr>
<td>default_address.country</td>
<td>Address.Country</td>
</tr>
<tr>
<td>default_address.zip</td>
<td>Address.PostalCode</td>
</tr>
</tbody>
</table>

Example

The following example shows how to map a source field to a target field.

```
"shopifyCustomerId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_profile.Attributes.ShopifyCustomerId"
}
```
The Shopify-Customer customer data from the Shopify object is associated with an Amazon Connect customer profile using the following index.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Shopify-Customer source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_shopifyCustomerId</td>
<td>id</td>
</tr>
</tbody>
</table>

For example, you can use _shopifyCustomerId as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Shopify-Customer objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectType set to Shopify-Customer.

**Object type mapping for the standard order**

The topics in this section provide the standard order definition, and the object type mapping from external applications to the standard order.

**Contents**

- Amazon AppIntegrations access requirements
- Amazon EventBridge access requirements
- Standard order definition
- Mapping Shopify objects to the standard order

**Amazon AppIntegrations access requirements**

Following are the Amazon AppIntegrations access requirements to create and delete Shopify integrations:

- app-integrations:GetEventIntegration
- app-integrations:ListEventIntegrationAssociations
- app-integrations:CreateEventIntegrationAssociation
- app-integrations:DeleteEventIntegrationAssociation
Amazon EventBridge access requirements

Following are the Amazon EventBridge access requirements to create and delete Shopify integrations:

- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:DeleteRule
- events:RemoveTargets

Standard order definition

The following table lists all the fields in the Customer Profiles standard order object.

<table>
<thead>
<tr>
<th>Standard order field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrderId</td>
<td>String</td>
<td>The unique identifier of a standard order.</td>
</tr>
<tr>
<td>CustomerEmail</td>
<td>String</td>
<td>The customer's email address.</td>
</tr>
<tr>
<td>CustomerPhone</td>
<td>String</td>
<td>The customer's phone number.</td>
</tr>
<tr>
<td>CreatedDate</td>
<td>String</td>
<td>The order's date created.</td>
</tr>
<tr>
<td>UpdatedDate</td>
<td>String</td>
<td>The order's date updated.</td>
</tr>
<tr>
<td>ProcessedDate</td>
<td>String</td>
<td>The order's date processed.</td>
</tr>
<tr>
<td>ClosedDate</td>
<td>String</td>
<td>The order's date closed.</td>
</tr>
<tr>
<td>CancelledDate</td>
<td>String</td>
<td>The order's date cancelled.</td>
</tr>
<tr>
<td>CancelReason</td>
<td>String</td>
<td>The order's cancel reason.</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>The order's name.</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AdditionalInformation</td>
<td>String</td>
<td>Any additional information relevant to the order.</td>
</tr>
<tr>
<td>Gateway</td>
<td>String</td>
<td>The order's payment gateway.</td>
</tr>
<tr>
<td>Status</td>
<td>String</td>
<td>The order's status.</td>
</tr>
<tr>
<td>StatusCode</td>
<td>String</td>
<td>The order's status code. Valid values: DRAFT</td>
</tr>
<tr>
<td>StatusUrl</td>
<td>String</td>
<td>The order's status URL.</td>
</tr>
<tr>
<td>CreditCardNumber</td>
<td>String</td>
<td>The customer's credit card last four digits.</td>
</tr>
<tr>
<td>CreditCardCompany</td>
<td>String</td>
<td>The customer's credit card company.</td>
</tr>
<tr>
<td>FulfillmentStatus</td>
<td>String</td>
<td>The order's fulfillment status.</td>
</tr>
<tr>
<td>TotalPrice</td>
<td>String</td>
<td>The order's total price.</td>
</tr>
<tr>
<td>TotalTax</td>
<td>String</td>
<td>The order's total tax.</td>
</tr>
<tr>
<td>TotalDiscounts</td>
<td>String</td>
<td>The order's total discounts.</td>
</tr>
<tr>
<td>TotalItemsPrice</td>
<td>String</td>
<td>The order's total items price.</td>
</tr>
<tr>
<td>TotalShippingPrice</td>
<td>String</td>
<td>The order's total shipping price.</td>
</tr>
<tr>
<td>TotalTipReceived</td>
<td>String</td>
<td>The order's total tip received.</td>
</tr>
<tr>
<td>Currency</td>
<td>String</td>
<td>The order's currency.</td>
</tr>
<tr>
<td>TotalWeight</td>
<td>String</td>
<td>The order's total weight.</td>
</tr>
<tr>
<td>BillingAddress</td>
<td>OrderAddress</td>
<td>The customer's billing address.</td>
</tr>
<tr>
<td>ShippingAddress</td>
<td>OrderAddress</td>
<td>The customer's shipping address.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>OrderItems</td>
<td>OrderItem list</td>
<td>The order's items.</td>
</tr>
<tr>
<td>Attributes</td>
<td>String-to-string map</td>
<td>Key-value pair of attributes of a standard order.</td>
</tr>
</tbody>
</table>

**OrderAddress data type**

<table>
<thead>
<tr>
<th>Standard order field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>The name associated with an order address.</td>
</tr>
<tr>
<td>Address1</td>
<td>String</td>
<td>The first line of an order address.</td>
</tr>
<tr>
<td>Address2</td>
<td>String</td>
<td>The second line of an order address.</td>
</tr>
<tr>
<td>Address3</td>
<td>String</td>
<td>The third line of an order address.</td>
</tr>
<tr>
<td>Address4</td>
<td>String</td>
<td>The fourth line of an order address.</td>
</tr>
<tr>
<td>City</td>
<td>String</td>
<td>The city of an order address.</td>
</tr>
<tr>
<td>County</td>
<td>String</td>
<td>The county of an order address.</td>
</tr>
<tr>
<td>State</td>
<td>String</td>
<td>The state of an order address.</td>
</tr>
<tr>
<td>Province</td>
<td>String</td>
<td>The province of an order address.</td>
</tr>
<tr>
<td>Country</td>
<td>String</td>
<td>The country of an order address.</td>
</tr>
</tbody>
</table>
PostalCode  String  The postal code of an order address.

OrderItem data type

<table>
<thead>
<tr>
<th>Standard order field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>String</td>
<td>The title of an order item.</td>
</tr>
<tr>
<td>Price</td>
<td>String</td>
<td>The price of an order item.</td>
</tr>
<tr>
<td>Quantity</td>
<td>String</td>
<td>The quantity of an order item.</td>
</tr>
</tbody>
</table>

Mapping Shopify objects to the standard order

This topic lists which fields in Shopify objects map to fields in the standard order object in Customer Profiles.

Shopify-DraftOrder object

For a list of all the fields in a Shopify-DraftOrder object see The DraftOrder object in the Shopify documentation.

Mapping a Shopify-DraftOrder object to a standard order

A subset of the fields in the Shopify-DraftOrder object map to the standard order object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-DraftOrder object to the standard order.

The StatusCode is ACTIVATED if order_status_url exists in the source. Otherwise, the StatusCode is DRAFT.

<table>
<thead>
<tr>
<th>Shopify-DraftOrder source field</th>
<th>Standard order target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Attributes.ShopifyOrderId</td>
</tr>
<tr>
<td>customer.id</td>
<td>Attributes.ShopifyCustomerId</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>note</td>
<td>AdditionalInformation</td>
</tr>
<tr>
<td>email</td>
<td>CustomerEmail</td>
</tr>
<tr>
<td>currency</td>
<td>Currency</td>
</tr>
<tr>
<td>created_at</td>
<td>CreatedDate</td>
</tr>
<tr>
<td>updated_at</td>
<td>UpdatedDate</td>
</tr>
<tr>
<td>name</td>
<td>Name</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
</tr>
<tr>
<td>order_status_url</td>
<td>StatusCode</td>
</tr>
<tr>
<td>billing_address.address1</td>
<td>BillingAddress.Address1</td>
</tr>
<tr>
<td>billing_address.address2</td>
<td>BillingAddress.Address2</td>
</tr>
<tr>
<td>billing_address.city</td>
<td>BillingAddress.City</td>
</tr>
<tr>
<td>billing_address.zip</td>
<td>BillingAddress.PostalCode</td>
</tr>
<tr>
<td>billing_address.province</td>
<td>BillingAddress.Province</td>
</tr>
<tr>
<td>billing_address.country</td>
<td>BillingAddress.Country</td>
</tr>
<tr>
<td>billing_address.name</td>
<td>BillingAddress.Name</td>
</tr>
<tr>
<td>shipping_address.address1</td>
<td>ShippingAddress.Address1</td>
</tr>
<tr>
<td>shipping_address.address2</td>
<td>ShippingAddress.Address2</td>
</tr>
<tr>
<td>shipping_address.city</td>
<td>ShippingAddress.City</td>
</tr>
<tr>
<td>shipping_address.zip</td>
<td>ShippingAddress.PostalCode</td>
</tr>
<tr>
<td>shipping_address.province</td>
<td>ShippingAddress.Province</td>
</tr>
<tr>
<td>shipping_address.country</td>
<td>ShippingAddress.Country</td>
</tr>
<tr>
<td>shipping_address.name</td>
<td>ShippingAddress.Name</td>
</tr>
<tr>
<td>invoice_url</td>
<td>StatusUrl</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>total_price</td>
<td>TotalPrice</td>
</tr>
<tr>
<td>total_tax</td>
<td>TotalTax</td>
</tr>
<tr>
<td>line_items[].title</td>
<td>OrderItems[].Title</td>
</tr>
<tr>
<td>line_items[].price</td>
<td>OrderItems[].Price</td>
</tr>
<tr>
<td>line_items[].quantity</td>
<td>OrderItems[].Quantity</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to map a source field to a target field.

```
"shopifyOrderId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_order.Attributes.ShopifyOrderId"
}
```

The Shopify-DraftOrder customer data from the Shopify object is associated with an Amazon Connect standard order using the following index.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Shopify-DraftOrder source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_shopifyOrderId</td>
<td>id</td>
</tr>
</tbody>
</table>

For example, you can use _shopifyOrderId as an ObjectFilter.KeyName with the the `ListProfileObjects` API to find a standard order. You can find the Shopify-DraftOrder objects associated with a specific profile by using the `ListProfileObjects` API with the ProfileId and ObjectTypeName set to Shopify-DraftOrder.

**Shopify-Order object**

For a list of all the fields in a Shopify-Order object see The Order object in the Shopify documentation.
## Mapping a Shopify-Order object to a standard order

A subset of the fields in the Shopify-Order object map to the standard order object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-Order object to the standard order.

The **StatusCode** is ACTIVATED if `order_status_url` exists in the source. Otherwise, the **StatusCode** is DRAFT.

<table>
<thead>
<tr>
<th>Shopify-Order source field</th>
<th>Standard order target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Attributes.ShopifyOrderId</td>
</tr>
<tr>
<td>customer.id</td>
<td>Attributes.ShopifyCustomerId</td>
</tr>
<tr>
<td>cancelled_at</td>
<td>CancelledDate</td>
</tr>
<tr>
<td>cancel_reason</td>
<td>CancelReason</td>
</tr>
<tr>
<td>closed_at</td>
<td>ClosedDate</td>
</tr>
<tr>
<td>created_at</td>
<td>CreatedDate</td>
</tr>
<tr>
<td>currency</td>
<td>Currency</td>
</tr>
<tr>
<td>email</td>
<td>CustomerEmail</td>
</tr>
<tr>
<td>financial_status</td>
<td>Status</td>
</tr>
<tr>
<td>order_status_url</td>
<td>StatusCode</td>
</tr>
<tr>
<td>fulfillment_status</td>
<td>FulfillmentStatus</td>
</tr>
<tr>
<td>gateway</td>
<td>Gateway</td>
</tr>
<tr>
<td>name</td>
<td>Name</td>
</tr>
<tr>
<td>note</td>
<td>AdditionalInformation</td>
</tr>
<tr>
<td>order_status_url</td>
<td>StatusUrl</td>
</tr>
<tr>
<td>Field</td>
<td>Mapping</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>phone</td>
<td>CustomerPhone</td>
</tr>
<tr>
<td>processed_at</td>
<td>ProcessedDate</td>
</tr>
<tr>
<td>total_discounts</td>
<td>TotalDiscounts</td>
</tr>
<tr>
<td>total_line_items_price</td>
<td>TotalItemsPrice</td>
</tr>
<tr>
<td>total_price</td>
<td>TotalPrice</td>
</tr>
<tr>
<td>total_shipping_price_set.shop_money.amount</td>
<td>TotalShippingPrice</td>
</tr>
<tr>
<td>total_tax</td>
<td>TotalTax</td>
</tr>
<tr>
<td>total_tip_received</td>
<td>TotalTipReceived</td>
</tr>
<tr>
<td>total_weight</td>
<td>TotalWeight</td>
</tr>
<tr>
<td>updated_at</td>
<td>UpdatedDate</td>
</tr>
<tr>
<td>billing_address.address1</td>
<td>BillingAddress.Address1</td>
</tr>
<tr>
<td>billing_address.address2</td>
<td>BillingAddress.Address2</td>
</tr>
<tr>
<td>billing_address.city</td>
<td>BillingAddress.City</td>
</tr>
<tr>
<td>billing_address.zip</td>
<td>BillingAddress.PostalCode</td>
</tr>
<tr>
<td>billing_address.province</td>
<td>BillingAddress.Province</td>
</tr>
<tr>
<td>billing_address.country</td>
<td>BillingAddress.Country</td>
</tr>
<tr>
<td>billing_address.name</td>
<td>BillingAddress.Name</td>
</tr>
<tr>
<td>payment_details.credit_card_number</td>
<td>CreditCardNumber</td>
</tr>
<tr>
<td>payment_details.credit_card_company</td>
<td>CreditCardCompany</td>
</tr>
<tr>
<td>shipping_address.address1</td>
<td>ShippingAddress.Address1</td>
</tr>
<tr>
<td>shipping_address.address2</td>
<td>ShippingAddress.Address2</td>
</tr>
<tr>
<td>shipping_address.city</td>
<td>ShippingAddress.City</td>
</tr>
</tbody>
</table>
Example

The following example shows how to map a source field to a target field.

```
"shopifyOrderId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_order.Attributes.ShopifyOrderId"
}
```

The Shopify-Order customer data from the Shopify object is associated with an Amazon Connect standard order using the following index.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Shopify-Order source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_shopifyOrderId</td>
<td>id</td>
</tr>
</tbody>
</table>

For example, you can use _shopifyOrderId as an ObjectFilter.KeyName with the ListProfileObjects API to find a standard order. You can find the Shopify-Order objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectTypeName set to Shopify-Order.

Object type mapping for the standard asset

The topics in this section provide the standard asset definition, and the object type mapping from external applications to the standard asset.
Contents

- Amazon AppFlow access requirements
- Standard asset definition
- Mapping Salesforce objects to the standard asset

Amazon AppFlow access requirements

Following are the Amazon AppFlow access requirements to create and delete Salesforce integrations:

- appflow:CreateFlow
- appflow:DeleteFlow

Standard asset definition

The following table lists all the fields in the Customer Profiles standard asset object.

<table>
<thead>
<tr>
<th>Standard asset field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetId</td>
<td>String</td>
<td>The unique identifier of a standard asset.</td>
</tr>
<tr>
<td>AssetName</td>
<td>String</td>
<td>The asset's name.</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>String</td>
<td>The asset's serial number.</td>
</tr>
<tr>
<td>ModelNumber</td>
<td>String</td>
<td>The asset's model number.</td>
</tr>
<tr>
<td>ModelName</td>
<td>String</td>
<td>The asset's model name.</td>
</tr>
<tr>
<td>ProductSKU</td>
<td>String</td>
<td>The asset's stock keeping unit.</td>
</tr>
<tr>
<td>PurchaseDate</td>
<td>String</td>
<td>The asset's purchase date.</td>
</tr>
<tr>
<td>UsageEndDate</td>
<td>String</td>
<td>The asset's usage end date.</td>
</tr>
<tr>
<td>Status</td>
<td>String</td>
<td>The asset's status.</td>
</tr>
<tr>
<td>Price</td>
<td>String</td>
<td>The asset's price.</td>
</tr>
<tr>
<td><strong>Standard asset field</strong></td>
<td><strong>Data type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Quantity</td>
<td>String</td>
<td>The asset's quantity.</td>
</tr>
<tr>
<td>Description</td>
<td>String</td>
<td>The asset's description.</td>
</tr>
<tr>
<td>AdditionalInformation</td>
<td>String</td>
<td>Any additional information relevant to the asset.</td>
</tr>
<tr>
<td>DataSource</td>
<td>String</td>
<td>The asset's data source.</td>
</tr>
<tr>
<td>Attributes</td>
<td>String-to-string map</td>
<td>Key-value pair of attributes of a standard asset.</td>
</tr>
</tbody>
</table>

**Mapping Salesforce objects to the standard asset**

This topic lists which fields in Salesforce objects map to fields in the standard asset object in Customer Profiles.

**Salesforce-Asset object**

Following is a list of all the fields in a Salesforce-Asset object.

- Id
- ContactId
- AccountId
- ParentId
- RootAssetId
- Product2Id
- ProductCode
- IsCompetitorProduct
- CreatedDate
- CreatedById
- LastModifiedDate
- LastModifiedById
- SystemModstamp
- IsDeleted
- Name
- SerialNumber
- InstallDate
- PurchaseDate
- UsageEndDate
- LifecycleStartDate
- LifecycleEndDate
- Status
- Price
- Quantity
- Description
- OwnerId
- AssetProvidedBy
- AssetServiceById
- IsInternal
- AssetLevel
- StockKeepingUnit
- HasLifecycleManagement
- CurrentMrr
- CurrentLifecycleEndDate
- CurrentQuantity
- CurrentAmount
- LastViewedDate
- LastReferencedDate

**Mapping a Salesforce-Asset object to a standard asset**

A subset of the fields in the Salesforce-Asset object map to the standard asset object in Customer Profiles.
The following table lists which fields can be mapped from the Salesforce-Asset object to the standard asset.

<table>
<thead>
<tr>
<th>Salesforce-Asset source field</th>
<th>Standard asset target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Attributes.sfdcAssetId</td>
</tr>
<tr>
<td>ContactId</td>
<td>Attributes.sfdcContactId</td>
</tr>
<tr>
<td>AccountId</td>
<td>Attributes.sfdcAccountId</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>SerialNumber</td>
</tr>
<tr>
<td>StockKeepingUnit</td>
<td>ProductSKU</td>
</tr>
<tr>
<td>UsageEndDate</td>
<td>UsageEndDate</td>
</tr>
<tr>
<td>Status</td>
<td>Status</td>
</tr>
<tr>
<td>Price</td>
<td>Price</td>
</tr>
<tr>
<td>Quantity</td>
<td>Quantity</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
</tr>
</tbody>
</table>

The Salesforce-Asset customer data from the Salesforce object is associated with an Amazon Connect standard asset using the indexes in the following table.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Salesforce-Asset source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_salesforceAssetId</td>
<td>Id</td>
</tr>
<tr>
<td>_salesforceContactId</td>
<td>ContactId</td>
</tr>
<tr>
<td>_salesforceAccountId</td>
<td>AccountId</td>
</tr>
</tbody>
</table>

For example, you can use _salesforceAssetId and _salesforceAccountId as an ObjectFilter.KeyName with the ListProfileObjects API to find a standard asset. You can find the Object type mapping definition details.
Salesforce-Asset objects associated with a specific profile by using the `ListProfileObjects` API with the ProfileId and ObjectType set to Salesforce-Asset.

**Object type mapping for the standard case**

The topics in this section provide the standard case definition, and the object type mapping from external applications to the standard case.

**Contents**

- Amazon AppFlow access requirements
- Standard case definition
- Mapping Zendesk objects to the standard case
- Mapping ServiceNow objects to the standard case

**Amazon AppFlow access requirements**

Following are the Amazon AppFlow access requirements to create and delete Zendesk and ServiceNow integrations:

- appflow:CreateFlow
- appflow:DeleteFlow

**Standard case definition**

The following table lists all the fields in the Customer Profiles standard case object.

<table>
<thead>
<tr>
<th>Standard case field</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CaseId</td>
<td>String</td>
<td>The unique identifier of a standard case.</td>
</tr>
<tr>
<td>Title</td>
<td>String</td>
<td>The case's title</td>
</tr>
<tr>
<td>Summary</td>
<td>String</td>
<td>The case's summary.</td>
</tr>
<tr>
<td>Status</td>
<td>String</td>
<td>The case's status.</td>
</tr>
<tr>
<td>Reason</td>
<td>String</td>
<td>The case's reason.</td>
</tr>
<tr>
<td>Standard case field</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>String</td>
<td>The case's creator.</td>
</tr>
<tr>
<td>CreatedDate</td>
<td>String</td>
<td>The case's date created.</td>
</tr>
<tr>
<td>UpdatedDate</td>
<td>String</td>
<td>The case's date updated.</td>
</tr>
<tr>
<td>ClosedDate</td>
<td>String</td>
<td>The case's date closed.</td>
</tr>
<tr>
<td>AdditionalInformation</td>
<td>String</td>
<td>Any additional information relevant to the case.</td>
</tr>
<tr>
<td>DataSource</td>
<td>String</td>
<td>The case's data source.</td>
</tr>
<tr>
<td>Attributes</td>
<td>String-to-string map</td>
<td>Key-value pair of attributes of a standard case.</td>
</tr>
</tbody>
</table>

**Mapping Zendesk objects to the standard case**

This topic lists which fields in Zendesk objects map to fields in the standard case in Customer Profiles.

**Zendesk-tickets object**

Following is a list of all the fields in a Zendesk-tickets object.

- id
- url
- type
- subject
- raw_subject
- description
- priority
- status
- recipient
- requester_id
- submitter_id
- assignee_id
- organization_id
- group_id
- collaborator_ids
- email_cc_ids
- follower_ids
- forum_topic_id
- problem_id
- has_incidents
- due_at
- tags
- via.channel
- custom_fields
- satisfaction_rating
- sharing_agreement_ids
- followup_ids
- ticket_form_id
- brand_id
- allow_channelback
- allow_attachments
- is_public
- created_at
- updated_at

**Mapping Zendesk-tickets object to a standard case**

A subset of the fields in the Zendesk-tickets object map to the standard case in Customer Profiles. The following table lists which fields can be mapped from the Zendesk-tickets object to the standard case.
<table>
<thead>
<tr>
<th>Zendesk-tickets source field</th>
<th>Standard case target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>requester_id</td>
<td>Attributes.ZendeskUserId</td>
</tr>
<tr>
<td>id</td>
<td>Attributes.ZendeskTicketId</td>
</tr>
<tr>
<td>subject</td>
<td>Title</td>
</tr>
<tr>
<td>description</td>
<td>Summary</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
</tr>
<tr>
<td>requester_id</td>
<td>CreatedBy</td>
</tr>
<tr>
<td>created_at</td>
<td>CreatedDate</td>
</tr>
<tr>
<td>updated_at</td>
<td>UpdatedDate</td>
</tr>
</tbody>
</table>

The Zendesk-tickets customer data from the Zendesk object is associated with a Amazon Connect standard case using the following indexes.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Zendesk-tickets source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_zendeskUserId</td>
<td>requester_id</td>
</tr>
<tr>
<td>_zendeskTicketId</td>
<td>id</td>
</tr>
</tbody>
</table>

For example, you can use _zendeskUserId and _zendeskTicketId as an ObjectFilter.KeyName with the ListProfileObjects API to find a standard case. You can find the Zendesk-tickets objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectTypeNome set to Zendesk_tickets.

Mapping ServiceNow objects to the standard case

This topic lists which fields in ServiceNow objects map to fields in the standard case in Amazon Connect Customer Profiles.
**Servicenow-task object**

Following is list of all the fields in a Servicenow-task object.

- `sys_id`
- `active`
- `activity_due`
- `additional_assignee_list`
- `approval`
- `approval_history`
- `approval_set`
- `assigned_to`
- `assignment_group`
- `business_duration`
- `business_service`
- `calendar_duration`
- `closed_at`
- `closed_by`
- `cmdb_ci.display_value`
- `cmdb_ci.link`
- `comments`
- `comments_and_work_notes`
- `company`
- `contact_type`
- `contract`
- `correlation_display`
- `active`
- `correlation_id`
- `delivery_plan`
- `delivery_task`
- description
- due_date
- escalation
- expected_start
- follow_up
- group_list
- impact
- knowledge
- location
- made_sla
- number
- opened_at
- opened_by.display_value
- order
- parent
- priority
- reassignment_count
- service_offering
- short_description
- sla_due
- state
- sys_class_name
- sys_created_by
- sys_created_on
- active
- sys_domain.global
- sys_domain.link
- sys_domain_path
- sys_mod_count
• sys_updated_by
• sys_updated_on
• time_worked
• upon_approval
• upon_reject
• urgency
• user_input
• watch_list
• work_end
• work_notes
• work_notes_list
• work_start

### Mapping Servicenow-task to a standard case

A subset of the fields in the Servicenow-task object map to the standard case in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-task object to the standard case.

<table>
<thead>
<tr>
<th>Servicenow-task source field</th>
<th>Standard case target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_id</td>
<td>Attributes.ServiceNowTaskId</td>
</tr>
<tr>
<td>opened_by.link</td>
<td>Attributes.ServiceNowSystemUserId</td>
</tr>
<tr>
<td>short_description</td>
<td>Title</td>
</tr>
<tr>
<td>description</td>
<td>Summary</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
</tr>
<tr>
<td>sys_created_by</td>
<td>CreatedBy</td>
</tr>
<tr>
<td>sys_created_on</td>
<td>CreatedDate</td>
</tr>
<tr>
<td>Servicenow-task source field</td>
<td>Standard case target field</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>sys_updated_on</td>
<td>UpdatedDate</td>
</tr>
</tbody>
</table>

The Servicenow-task customer data from Servicenow is associated with an Amazon Connect standard case using the indexes in the following table.

<table>
<thead>
<tr>
<th>Standard Index Name</th>
<th>Servicenow-task source field</th>
</tr>
</thead>
<tbody>
<tr>
<td>_serviceNowTaskId</td>
<td>sys_id</td>
</tr>
<tr>
<td>_serviceNowSystemId</td>
<td>open_by.link</td>
</tr>
</tbody>
</table>

For example, you can use _serviceNowTaskId and _serviceNowSystemId as an ObjectFilter.KeyName with the ListProfileObjects API to find a standard case. You can find the Servicenow-task objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectTypeName set to Servicenow-task.

**Servicenow-incident object**

Following is a list of all the fields in a Servicenow-incident object.

- sys_id
- business_stc
- calendar_stc
- caller_id.link
- caller_id.value
- category
- caused_by
- child_incidents
- close_code
- hold_reason
- incident_state
- notify
- parent_incident
- problem_id
- reopened_by
- reopened_time
- reopen_count
- resolved_at
- reopened_by.link
- reopened_by.value
- rfc
- severity
- subcategory

**Mapping Servicenow-incident to a standard case**

A subset of the fields in the Servicenow-incident object map to the standard case in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-incident object to the standard case.

<table>
<thead>
<tr>
<th>Servicenow-incident source field</th>
<th>Standard case target field</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_id</td>
<td>Attributes_ServiceNowIncidentId</td>
</tr>
<tr>
<td>caller_id.link</td>
<td>Attributes_ServiceNowSystemUserId</td>
</tr>
<tr>
<td>incident_status</td>
<td>Status</td>
</tr>
<tr>
<td>caller_id.link</td>
<td>CreatedBy</td>
</tr>
<tr>
<td>resolved_at</td>
<td>ClosedDate</td>
</tr>
<tr>
<td>category</td>
<td>Reason</td>
</tr>
</tbody>
</table>

The Servicenow-incident customer data from the Servicenow object is associated with an Amazon Connect standard case using the indexes in the following table.
For example, you can use _serviceNowIncidentId and _serviceNowSystemId as a ObjectFilter.KeyName with the ListProfileObjects API to find a standard case. You can find the Servicenow-incident objects associated with a specific profile by using the ListProfileObjects API with the ProfileId and ObjectTypeNamset to Servicenow-incident.

### Additional properties of object types

A property type defines which key should be used to encrypt any data of the object type.

There is an option that defines if new profiles can be created by the ingestion of this object. Normally when an object is ingested that cannot be matched to an existing profile, a new profile is created as long as this option is true. If it is not true then the ingested object is created and written to the domain dead-letter queue.

It also contains how long data of this object type should be retained in Customer Profiles.

#### Note

Retention on individual objects is set at the time of ingestion of data. Changing the retention for a specific object type only applies to new data being ingested. It does not apply to existing data already ingested.

### Inferred profiles

When a profile is created by the ingestion of an object that has no fields, the standard profile object of this new profile is empty. This empty standard profile object is an inferred profile.

When creating an inferred profile, the following two fields are populated in the standard object from the profile object, if available.

- If there is any field defined with the content type of EMAIL_ADDRESS in the ingested object then this value will be populated into the EmailAddress field of the standard profile.
• If there is any field with the content type of PHONE_NUMBER in the ingested object then this value will be populated into the PhoneNumber field of the standard profile.

Values for these fields are populated into the standard profile even if the fields do not have a target defined in the field definition.

**Contact record templates**

What is a Contact Record? A Contact Record serves as a profile object that captures essential meta-data from various contact events, such as phone calls or chats. It plays a vital role in documenting and analyzing interactions with customers. When a contact event takes place, we offer three distinct default templates that can be applied to your domain. These templates serve as configuration options, governing how the contact event is handled within the system. Each template defines specific rules and actions, allowing you to tailor the processing of contact events according to your business needs.

### Create inferred profiles and auto-associate profiles (CTR-NoInferred)

**Description**

When the CTR-NoInferred template is utilized and a contact event, such as a phone call takes place, a specific process is initiated to handle the data. Initially, the system uses the _ctrContactId key to search for an existing profile associated with the contact event. If a matching profile is found, the contact event is automatically associated with that profile. However, if no existing profile is found using the _ctrContactId key, the system proceeds to search for a profile using a secondary key called _phone. This key is used to locate an existing profile based on the phone number associated with the contact event. When a matching profile is found, the contact event is automatically associated with that profile.

In cases where neither the _ctrContactId key nor the _phone key yield an existing profile, the system creates a new inferred profile. This inferred profile is then populated with the meta-data from the contact event, ensuring that the information is captured and stored within the system.

This process ensures efficient handling of contact events, promoting auto-association with existing profiles and enabling the creation of inferred profiles when necessary. By leveraging these mechanisms, organizations can maintain a comprehensive record of customer interactions and effectively manage their contact event data within the system.
It is recommended to use the CTR-NoInferred template as the default behavior due to its significant advantages, especially in reducing duplicate profiles.

**Auto-associate profiles only (CTR-AutoAssociateOnly)**

**Description**

The CTR-AutoAssociateOnly template functions similarly to the CTR-NoInferred template with one important distinction: it does not create an inferred profile when no existing profile can be found for auto-association.

When a contact event, such as a phone call, takes place, the CTR-AutoAssociateOnly template utilizes the `_ctrContactId` key to search for a matching existing profile. If a profile is found, the contact event is automatically associated with that profile.

However, if no existing profile is found using the `_ctrContactId` key, the template employs a secondary search mechanism using the `_phone` key. It searches for an existing profile associated with the same phone number as the contact event. If a matching profile is found, the contact event is auto-associated with that profile.
The purpose of using the CTR-AutoAssociateOnly template is to enable automatic association with existing profiles while maintaining strict control over profile creation. Unlike the CTR-NoInferred template, this template prevents the creation of inferred profiles when no match is found. It ensures that profiles are only created manually, providing organizations with a higher level of control and accuracy in profile management.

By utilizing the CTR-AutoAssociateOnly template, organizations can leverage auto-association while adhering to specific rules regarding profile creation. This approach allows for streamlined contact event handling and precise control over the profile ecosystem, ensuring accurate data representation and facilitating efficient customer management.

Create inferred profiles only (CTR)

Description

The CTR template relies solely on the _ctrContactId key to search for an existing profile, and it automatically associates the contact event with the profile if a match is found. However, in cases where no existing profile is found, the template creates an inferred profile and populates it with the contact event meta-data.
Although this behavior ensures that contact events are captured even when no pre-existing profile exists, it can potentially result in the creation of numerous inferred profiles. This abundance of inferred profiles may lead to the issue of duplicate profiles within the system.

To address this concern and promote better profile management practices, we highly recommend utilizing the CTR-NoInferred template as the default option. By using the CTR-NoInferred template, the system eliminates the creation of inferred profiles, thereby reducing the occurrence of duplicate profiles. This template allows for a more streamlined and efficient handling of contact events, resulting in improved data integrity and accuracy.

By adopting the CTR-NoInferred template as the default choice, organizations can optimize their profile management processes, minimize data duplication, and ensure a more reliable representation of customer interactions.

**Contact record template usage examples**

**Amazon Connect admin center**

- In the console UI, when creating a new domain, you have the option to select the desired CTR behavior. This can be done through the radio button options available in the **Profile creation**
and auto-association section. Similarly, when selecting an existing domain, the radio button option will reflect the behavior previously associated with that domain.

- When editing a currently enabled domain, the Domain details page will display the currently applied behavior in the Profile creation and auto-association section. By choosing the Edit button in the header of this section, you will be redirected to the Edit Profile creation and auto-association page. Here, you can choose a different behavior according to your requirements.

- Alternatively, if you are viewing the CTR mapping from the Data mapping page, you can choose the Change template button. This action will also take you to the Edit Profile creation and auto-association page, where you can select a different behavior that suits your needs.

These options provide you with flexibility in managing the CTR behavior for your domains, allowing you to easily customize and modify the settings based on your specific preferences or evolving business requirements.

AWS CLI

- To use the CTR-NoInferred template, run the following command on the CLI:

  ```bash
  aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "Creates inferred profiles and auto-associates profiles" --template-id CTR-NoInferred
  ```

- To use the CTR-AutoAssociateOnly template, run the following command on the CLI:

  ```bash
  aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "Auto-associate with profiles only" --template-id CTR-AutoAssociateOnly
  ```

- To use the CTR template, run the following command on the CLI:

  ```bash
  aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "Creates inferred profiles only" --template-id CTR
  ```

API

For information on using the API, see PutProfileObjectType
Automatically associate the Contact Record with one profile found using the _phone key

You can automatically associate the Contact Record with one profile found using the _phone key.

Example

In the domain, the following profile is created by the CreateProfile API:

```json
{
    "FirstName": "John",
    "LastName": "Doe",
    "PhoneNumber": "+11234567890"
}
```

When a call is received from the PhoneNumber +11234567890 using the default CTR template, the Contact Record will not be automatically associated with the above profile unless an agent has already manually associated the Contact Record with the same caller to the above profile. If the Contact Record was not associated manually or automatically, Customer Profiles will create an inferred profile with the information from the Contact Record.

To automatically associate the above profile with contact records without manual agent intervention, you can use the CTR-NoInferred template. When a call is received from the PhoneNumber +11234567890 using the CTR-NoInferred template, the Contact Record will automatically associate with the above profile using the _phone profile key.

There are two scenarios in which Customer Profiles will not be able to automatically associate Contact Records to a profile:

- If more than one profile is found using the _phone profile key, Customer Profiles cannot associate the Contact Record to a unique profile and the request will be rejected.
- If no profile is found for the _phone profile key, Customer Profiles will create an inferred profile.

To use the CTR-NoInferred template to replace the default CTR template, run the following command on the CLI:
aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "No inferred contact record profiles" --template-id CTR-NoInferred

To revert to the default behavior, run the following command on the CLI:

aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "Revert to inferred contact record profiles" --template-id CTR

**Examples of object type mappings**

**An object type mapping that generates a profile**

The following example shows data that populates the standard profile.

Following is the incoming object:

```json
{
    "account": 1234,
    "email": "john@examplecorp.com",
    "address": {
        "address1": "Street",
        "zip": "Zip",
        "city": "City"
    },
    "firstName": "John",
    "lastName": "Doe"
}
```

The following code shows that incoming object mapping into a standard profile object and indexing `PersonalEmailAddress`, `fullName`, and `accountId`, which is a unique key.

```json
{
    "Fields": {
        "accountId": {
            "Source": "_source.account",
            "Target": "_profile.AccountNumber",
            "ContentType": "NUMBER"
        },
        "shippingAddress.address1": {
```
Examples of object type mappings

```
"source": "_source.address.address1",
"target": "_profile.ShippingAddress.Address1"
},
"shippingAddress.postalCode": {
  "source": "_source.address.zip",
  "target": "_profile.ShippingAddress.PostalCode"
},
"shippingAddress.city": {
  "source": "_source.address.city",
  "target": "_profile.ShippingAddress.City"
},
"personalEmailAddress": {
  "source": "_source.email",
  "target": "_profile.PersonalEmailAddress",
  "contentType": "EMAIL_ADDRESS"
},
"fullName": {
  "source": "{{_source.firstName}} {{_source.lastName}}"
},
"firstName": {
  "source": "_source.firstName",
  "target": "_profile.FirstName"
},
"lastName": {
  "source": "_source.lastName",
  "target": "_profile.LastName"
}
},
"keys": {
  "_email": [
    {
      "fieldNames": ["personalEmailAddress"]
    }
  ],
  "_fullName": [
    {
      "fieldNames": ["fullName"]
    }
  ],
  "_account": [
    {
      "standardIdentifiers": ["PROFILE","UNIQUE"],
      "fieldNames": ["accountId"]
    }
  ]
}
```
Note that email and fullname are indexed, but they aren't used to search for the profile. The account is the unique key. It is required to specify the object. Any time an object with the same account ID is ingested it overwrites the previous object with the same account ID.

Several fields are populated in the standard profile object (see the fields that have Target defined).

**An object type mapping that doesn't populate the standard profile**

This example shows a more complicated use case. It ingests data related to a profile but it doesn't necessarily populate the standard profile object.

Following is the incoming object:

```json
{
  "email": "john@examplecorp.com",
  "timestamp": "2010-01-01T12:34:56Z",
  "subject": "Whatever this is about",
  "body": "Body of ticket"
}
```

Following is one way of mapping this data:

```json
{
  "Fields": {
    "email": {,
      "Source": "_source.email",
      "ContentType": "EMAIL_ADDRESS"
    },
    "timestamp": {
      "Source": "_source.timestamp"
    }
  },
  "Keys": {
    "_email": [,
      {
        "StandardIdentifiers": ["PROFILE","LOOKUP_ONLY"],
        "FieldNames": ["email"]
      }
    ]
  }
}
```

Examples of object type mappings
This example ingests the data and, at first lookup, it ingests the email address.

- If the email address matches a single profile, it is used to attach the data to that specific profile. The unique identifier for the ticket is comprised of the email and the timestamp since no other unique identifier exists.

- If no profile exists with the specified email, a new profile is created with the single field of EmailAddress filled in. The ingested object is attached to this new inferred profile. The two searchable keys that can find the profile are _email and uniqueTicket.

- If more than one profile exists with the specified email address, a new profile is created with the single field of EmailAddress filled in and the object is attached to this new profile. This profile is created with the ticketEmail key defined, in addition to _email and uniqueTicket. Any subsequent tickets from that email are assigned to this new inferred profile. The reason for this is that the _email key is referring to three profiles and is thus discarded, however the ticketEmail key only refers to a single profile (the new inferred one) and is still valid.

- In cases where a new inferred profile is created, the EmailAddress field is populated from the first object that created it.

**Implicit profile object types**

You can use any object type that matches the name of a template ID (as returned by the ListProfileObjectTypeTemplates API) without explicitly defining it. The object type will exactly
match the definition of the template definition of this object type. If an explicit object type is defined, it replaces the implicit one.

Implicit object types are included in the ListProfileObjectTypes API or returned by GetProfileObjectType operations, but they can still be deleted if you want to remove all data ingested from that object type.

**Generative AI powered data mapping**

Amazon Connect Customer Profiles provides a generative AI powered customer data mapping capability that significantly reduces the time needed to create unified profiles, enabling you to help provide more personalized customer experiences.

With this capability, when contact center administrators add customer data from any of the 70+ available no-code data connectors such as Adobe Analytics, Salesforce, or Amazon Simple Storage Service (S3), Amazon Connect Customer Profiles will analyze the data from these sources to automatically determine how to organize and combine data that exists in different formats across disparate sources into unified profiles in Amazon Connect. With just a few clicks, contact center administrators can review and complete the setup of customer profiles so they can provide agents with relevant customer information and dynamically personalize IVRs and chatbots to improve customer satisfaction and agent productivity.

Generative AI powered customer data mapping is available in the following regions:

- US East (N. Virginia)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Canada (Central)
- Europe (Frankfurt)
- Europe (London)
Set up generative AI powered data mapping

1. Open the Amazon Connect Customer Profiles console.
2. On the **Data source integrations** tab, choose **Add data source integration**.
3. Set up the connection. Select the data source from drop-down that has all supported connectors available.

4. Map data. Select the option to auto-generate data mapping, or select an already existing mapping template or create one from scratch.
5. Review mapping summary. Review the auto-generated mapping results summary that shows all the customer attributes. Make edits to ingestion keys and confirm before starting data ingestion.
How it works

The system works in four phases. In the first phase, Customer Profiles fetches source attributes and, if available, samples data from your data source, subsequently determining the most appropriate object type for the target. For an Amazon S3 data source, the first CSV file found...
in the selected Amazon S3 bucket and prefix will be used as the sample data. For other data sources, Customer Profiles fetches source attributes through AppFlow. In the second phase, a large language model (LLM) is leveraged to further process each of the custom attributes and map them to standard customer profile attributes. LLM is used again in the third phase to select the suitable attributes that can serve as keys, such as customer identifiers. Finally in the fourth phase, the timestamp format detector parses the timestamps to maintain the right chronological order of the records. The system is able to generate the mapping for up to 120 attributes in less than 20 seconds after combining the prediction results.

**Generative AI powered data mapping troubleshooting**

The following sections display the possible error messages that you may encounter. It also provides the cause and resolution for each issue.

**Error: Could not parse object string into JSON**

The object string in the request is not a valid JSON. Review the object string in the request and verify that it is valid JSON.

**Error: Value at 'objects' failed to satisfy constraint: Member must have length less than or equal to 5**

There are too many objects in the request. Up to five objects are allowed in a request. Reduce the number of objects to five or less.

**Error: Breached limit of 120 attributes**

Up to 120 attributes are allowed in a JSON object, including nested JSON attributes. Remove some attributes that don't need to be mapped from the JSON object.
Warning: We couldn't find a unique key, which distinguishes your data. We couldn't find a profile key, which identifies your profiles.

The model could not find a valid object type from given object. Change the input or use manual mapping approach as suggested.

Create and ingest customer data into Customer Profiles by using Amazon S3

You can define data from any source using Amazon S3 and seamlessly enrich a customer profile without the need for custom or pre-built integrations. For example, say you want to provide agents with relevant purchase history information. You can import purchase transaction data from an internal application into a spreadsheet file on S3 and then link it to a customer profile.

To set this up, you need to define an object type mapping that describes what the custom profile object looks like. This mapping defines how fields from your data can be used to either populate fields in the standard profile or how it can be used to assign the data to a specific profile.

After you create the object type mapping, you can use the PutProfileObject API to upload the custom profile data from your CRM into the custom profile object.

Note
Customer Profiles does not support ingesting data from CSV headers that contain dot notation.
Set up real-time export

Amazon Connect Customer Profiles provides real-time data export of unified customer profiles to an Amazon Kinesis Data Stream. You can enable data streaming and automatically receive data for new profiles and updates to existing profiles into your Amazon Kinesis Data Stream.

You can keep your source systems data, such as CRMs and marketing automation tools, up-to-date with the latest information from Amazon Connect Customer Profiles. For example, when a customer calls your contact center to update their address, an agent can make the change to add the new customer address, and the updated profile information is sent to a Kinesis Data Stream in real-time.

To set this up, you need to enable **Data export** in the Customer Profiles console.

Enable real-time export

To enable data streaming for your domain

1. Open the Amazon Connect Customer Profiles console.
2. Select the **Data export** tab and choose **Enable data streaming**

3. Choose **Enable data streaming** and select an existing Kinesis data stream from the drop-down menu, or choose **create a new Kinesis data stream** to open the Kinesis console and create the stream. For more information, see [Creating and Managing Streams](#).
4. Choose the **Enable data streaming** button to save your settings.

**Enable real-time export**

**To disable data streaming for your domain**

1. Open the Amazon Connect Customer Profiles console.
2. Select the **Data export** tab and choose **Disable data streaming**.
Real-time export Kinesis payload

Sample output event in JSON

```json
{
    "SchemaVersion": 0,
    "EventId": "eventId",
    "EventTimestamp": "2020-01-01T00:00:00Z",
    "EventType": "CREATED",
    "DomainName": "domainName",
    "ObjectTypeName": "objectTypeName",
    "AssociatedProfileId": "associatedProfileId",
    "ProfileObjectUniqueKey": "profileObjectUniqueKey",
    "Object": {
        "map": {
            "k1": [
                "a",
                "b",
                "c"
            ]
        }
    },
    "IsMessageRealTime": true
}
```

**SchemaVersion**

The current version of the schema.

**EventId**

The unique event ID.

**EventTimestamp**

Timestamp of the event using the ISO8601 standard.

**EventType**

The type of event exported.

**Values**: CREATED, UPDATED, HEALTH_CHECK

- CREATED: The export event was for CreateProfile.
• **UPDATED**: The export event was for a UpdateProfile.
• **HEALTH_CHECK**: The export event was for a HealthCheck event to make sure Customer Profiles could successfully putEvent in Kinesis Stream.

**DomainName**

The domain the event belongs to. /Domain of the event

**ObjectTypeName**

Object type of the event

Values: _profile, _asset, _order, _case. You can also use predefined template name such as Salesforce-Account or a custom defined object name that you can create using the [PutProfileObjectType](#) API.

**AssociatedProfileId**

ID of the Standard Profile that the Object is associated to. It is only present if the object type is not _profile

**ProfileObjectUniqueKey**

The unique identifier of the ProfileObject generated by the service.

Type: String

**Object**

The Standard Profile or Standard Profile Object itself.

**IsMessageRealTime**

Flag to inform if the message is real-time or was re-driven.

**Sample payload in JSON**

```
{
   "SchemaVersion": 0,
   "EventId": "6049bf39-0000-0000-0000-b75656dd51a8",
   "EventTimestamp": "2023-02-24T07:17:05.356Z",
   "EventType": "UPDATED",
   "DomainName": "SampleDomain",
   "ObjectTypeName": "Salesforce-Account",
   "Real-time export Kinesis payload": 1992
}
```
Real-time export troubleshooting

When there is an issue sending events to the destination Kinesis Data Stream, the streaming can enter an error state.

The following sections display the possible error messages that you may encounter. It also provides the cause and resolution for each issue.
**Error: The Kinesis Data Stream is not Active. Please check the configuration and recreate the event stream later**

The destination Kinesis Data Stream is not in ACTIVE state. This can happen when your Kinesis Data Stream is being created or being deleted. To resolve the error, make sure your Kinesis Data Stream is in ACTIVE state and re-enable the data streaming setting.

**Error: The Kinesis Data Stream does not exist. Please recreate the event stream with valid Kinesis Data Stream destination**

The destination Kinesis Data Stream is deleted. To resolve the error, re-enable data streaming with an existing Kinesis Data Stream as the destination.

**Error: The Kinesis Data Stream is being throttled. Please consider provision higher Kinesis throughput appropriately**

The destination Kinesis Data Stream is being throttled (under-provisioned). To resolve the error, make sure the destination Kinesis Data Stream has enough shard count and then re-enable data streaming.

**Error: The KMS key used to encrypt Kinesis Data Stream is being throttled. Please consider increasing the KMS request quota appropriately**

The KMS key used by Kinesis Data Stream is being throttled. To resolve the error, re-enable data streaming.

**Error: Check the KMS Key configuration of you Kinesis Data Stream**

Customer Profiles cannot access the KMS key used by Kinesis Data Stream. This can happen when your KMS key has a key policy that denies access from Customer Profiles service-linked role, or the key is not in Enabled status. To resolve the error, make sure the KMS key policy does not deny access from Customer Profiles service-linked role, and the key is in Enabled status. Re-enable data streaming to resolve the error.

**Delete Customer Profiles domain**

Deleting mappings will only delete objects and data associated with that specific mapping. If there are multiple objects associated with a profile, then deleting a specific mapping may not clear the
profile data. If you want to delete specific data, you would then delete the mapping, but your profiles may still exist if they contain data from other mappings. This could result in additional charges for the existing profiles. To avoid this from occurring, you can delete your Customer Profiles domain using the Amazon Connect console by following these steps.

1. Login to the Amazon Connect console and select Customer Profiles from the left navigation pane. Choose your Customer Profiles domain and then choose View details.

2. Choose Delete domain.

3. To delete your domain, enter confirm in the box and choose Delete domain.
Customer Profiles Calculated Attributes

Amazon Connect Customer Profiles support the creation of calculated attributes which enables companies to define their own business logic to transform their customer profile data into actionable data points to personalize automated experiences such as interactive voice responses.

By using calculated attributes, companies can identify key attributes about their customer's past behaviour (such as the last website visited or last agent spoken to), patterns of behaviour (such as preferred channel, frequency of contact), and customer value (such as new customer, average ticket
Companies can use the calculated attributes API to create a new attribute using common aggregation operations such as average, count, minimum, maximum, and sum.

Calculated attributes automatically transforms raw data in real-time into actionable data points and metrics. Contact center administrators are able to define and configure calculations based on the raw data available in customer profiles. These calculated attributes make it easier for you to build automated experiences such as Interactive Voice Response (IVR) or chatbots. You can build personalized experiences and help agents understand customer context faster.

The calculated attributes API is available in the following regions:

- US East (N. Virginia)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Canada (Central)
- Europe (Frankfurt)
- Europe (London)

## Contents

- Calculated Attributes APIs
- Creating a custom calculated attribute definition
- Validating calculated attribute values using the API
- Default Calculated Attributes
- Error state and troubleshooting

## Calculated Attributes APIs

You can use the following Customer Profiles calculated attribute APIs
Create a new calculated attribute. This requires an existing object type in the domain. You can define attributes that you want to pull from a single source object and the mathematical operations to apply to them in aggregate as well as the time range and object count.

After creation, new object data ingested into Customer Profiles will be included in the calculated attribute, which can be retrieved for a profile using the GetCalculatedAttributeForProfile API. Defining a calculated attribute makes it available for all profiles within a domain. Each calculated attribute can only reference one ObjectType and at most two fields from that ObjectType.

**Request**

```
POST /domains/DomainName/calculated-attributes/CalculatedAttributeName
```

```
{
   "CalculatedAttributeName": "string",
   "DisplayName": "string",
   "Description": "string",
   "AttributeDetails": {
      "Attributes": [
         {
            "Name": "string"
         },
         ...
      ],
      "Expression": "string",
   },
   "Statistic": "AVERAGE" | "COUNT" | "SUM" | "FIRST_OCCURRENCE" | "LAST_OCCURRENCE" | "MINIMUM" | "MAXIMUM" | "MAX_OCCURRENCE",
   "Conditions": {
      "Range": {
         "Value": "number",
         "Units": "string"
      },
      "ObjectCount": "number",
      "Threshold": {
```
Response

```json
{
    "CalculatedAttributeName": "string",
    "DisplayName": "string",
    "Description": "string",
    "AttributeDetails": {
        "Attributes": [
            {
                "Name": "string"
            }
        ],
        "Expression": "string",
    },
    "Statistic": "AVERAGE" | "COUNT" | "SUM" | "FIRST_OCCURRENCE" | "LAST_OCCURRENCE" | "MINIMUM" | "MAXIMUM" | "MAX_OCCURRENCE",
    "Conditions": {
        "Range": {
            "Value": "number",
            "Units": "string"
        },
        "ObjectCount": "number",
        "Threshold": {
            "Value": "string",
            "Operator": "EQUAL_TO" | "GREATER_THAN" | "LESS_THAN" | "NOT_EQUAL_TO"
        }
    },
    "CreatedAt": number,
    "LastUpdatedAt": number,
    "Tags": {}
}
```
Request body

- **CalculatedAttributeName**

  The unique (per domain) name of the calculated attribute.
  - Type: String
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: ^[a-zA-Z0-9_-]+$
  - Required: Yes

- **DisplayName**

  The display name of the calculated attribute.
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: ^[a-zA-Z_][a-zA-Z_0-9-_]*$
  - Required: No

- **Description**

  The description of the calculated attribute.
  - Type: String
  - Required: No

- **AttributeDetails**

  Details of the attributes used in the definition and the mathematical operations involved between the attributes. See the following components:

  - **Attributes**

    A list of attribute items specified in the mathematical expression.

    - **AttributItem**

      The details of a single attribute item specified in the mathematical expression.
      - Name
        - The name of an attribute defined in a profile object type.
      - Expression
Mathematical expression that is performed on attribute items provided in the attribute list. Each element in the expression should follow the structure of \"{ObjectName.AttributeName}\".

- **Example**: \{ObjA.AttributeA\} - \{ObjA.AttributeB\}
- **Type**: String
- **We only support the following mathematical operations**: + - * /
- **You cannot make modifications to the Expression once a calculated attribute definition is created**

- **Conditions**

  Defines the calculated attribute aggregation criteria and threshold.
  - **Type**: Conditions object
    - **Range**
      - **ObjectCount**
      - **Threshold**

- **Range**

  The relative time period over which data is included in the aggregation.
  - **Type**: Range object
    - **Value**: The length of time of the specified units
    - **Unit**: Unit of time
      - **Valid values**: Days
    - **Required**: Yes
    - **Initial scope**: Max of 366 days

- **ObjectCount**

  The number of profile objects used for the calculated attribute.
  - **Type**: Number
  - **Range**: 1 through 100
  - **Required**: No

- **Threshold**

  The comparison logic to generate a true/false calculated attribute.
- **Type:** Threshold object
  - **Value**
    - The value of the threshold
    - **Type:** String
    - **Required:** No
  - **Operator**
    - The operator of the threshold
    - **Type:** ENUM
    - **Valid Values:**
      - GREATER_THAN
      - LESS_THAN
      - EQUAL_TO
      - NOT_EQUAL_TO
    - **Required:** No
  - **Statistic**
    - The aggregation operation to perform for the calculated attribute.
    - **Type:** ENUM
    - **Valid Values:**
      - FIRST_OCCURRENCE
      - LAST_OCCURRENCE
      - COUNT
      - SUM
      - MINIMUM
      - MAXIMUM
      - AVERAGE
      - MAX_OCCURRENCE

UpdateCalculatedAttributeDefinition
Update a calculated attribute definition. Updates are limited to display name, description, time range, object count, and threshold. This API supports partial updates, so only the parameters that require updating need to be included.

When updating the Conditions, note that increasing the date range of a calculated attribute will not trigger inclusion of historical data greater than the current date range.

**Request**

```
PUT /domains/DomainName/calculated-attributes/CalculatedAttributeName
```

```
{
    "DisplayName": "string",
    "Description": "string",
    "Conditions": {
        "Range": {
            "Value": "number",
            "Units": "string"
        },
        "ObjectCount": "number",
        "Threshold": {
            "Value": "string",
            "Operator": "EQUAL_TO" | "GREATER_THAN" | "LESS_THAN" | "NOT_EQUAL_TO"
        }
    }
}
```

**Response**

```
{
    "CalculatedAttributeName": "string",
    "DisplayName": "string",
    "Description": "string",
    "AttributeDetails": {
        "Attributes": [ { "Name": "string"
    }
}
```
Request body

- **DisplayName**

  The display name of the calculated attribute.

  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: ^[a-zA-Z_][a-zA-Z_0-9-\s]*$
  - Required: No

- **Description**

  The description of the calculated attribute.

  - Type: String
  - Required: No

- **Conditions**

  Defines the calculated attribute aggregation criteria and threshold.
- **Type**: Conditions object
  - Range
  - ObjectCount
  - Threshold

- **Range**

  The relative time period over which data is included in the aggregation.
  - **Type**: Range object
    - Value: The length of time of the specified units
    - Unit: Unit of time
      - Valid values: Days
  - **Required**: Yes
  - **Initial scope**: Max of 366 days

- **ObjectCount**

  The number of profile objects used for the calculated attribute.
  - **Type**: Number
  - **Range**: 1 through 100
  - **Required**: No

- **Threshold**

  The comparison logic to generate a true/false calculated attribute.
  - **Type**: Threshold object
    - Value
      - The value of the threshold
      - **Type**: String
      - **Required**: No
    - Operator
      - The operator of the threshold
      - **Type**: ENUM
        - **Valid Values**:
          - GREATER_THAN
• LESS_THAN
• EQUAL_TO
• NOT_EQUAL_TO

• Required: No

GetCalculatedAttributeDefinition

GetCalculatedAttributeDefinition

Retrieve a calculated attribute definition.

Request

GET /domains/DomainName/calculated-attributes/CalculatedAttributeName

Request Body

The request does not have a request body.

Response

{
    "CalculatedAttributeName": "string",
    "DisplayName": "string",
    "Description": "string",
    "AttributeDetails": {
        "Attributes": [
            {
                "Name": "string"
            }
        ]
    },
    "Expression": "string",
    "Statistic": "AVERAGE" | "COUNT" | "SUM" | "FIRST_OCCURRENCE" | "LAST_OCCURRENCE" | "MINIMUM" | "MAXIMUM" | "MAX_OCCURRENCE"
    "Conditions": {
        "Range": {

Calculated Attributes APIs

2006
URI request parameters

- **DomainName**

  The unique name of the domain.
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: `^[a-zA-Z0-9_\-]+$`
  - Required: Yes

- **CalculatedAttributeName**

  The unique (per domain) name of the calculated attribute.
  - Type: String
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: `^[a-zA-Z0-9_\-]+$`
  - Required: Yes

**DeleteCalculatedAttributeDefinition**

Delete an existing calculated attribute definition. Note that deleting a default calculated attribute is possible, however once deleted you will be unable to undo that action and will need to recreate it on your own using the `CreateCalculatedAttributeDefinition` API if you want it back.
Request

DELETE /domains/DomainName/calculated-attributes/CalculatedAttributeName

Request Body

The request does not have a request body.

Response

The response does not have a response body.

URI request parameters

- DomainName
  - The unique name of the domain.
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: ^[a-zA-Z0-9_-]+$
  - Required: Yes

- CalculatedAttributeName
  - The unique (per domain) name of the calculated attribute.
  - Type: String
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  - Pattern: ^[a-zA-Z0-9_-]+$
  - Required: Yes

ListCalculatedAttributeDefinitions

Retrieve all calculated attribute definitions for a domain.

Request
GET /domains/DomainName/calculated-attributes?max-results=MaxResults&next-token=NextToken

Request Body

The request does not have a request body.

Response

```
{
"Items": [
{
"CalculatedAttributeName": "string",
"DisplayName": "string",
"Description": "string",
"CreatedAt": "timestamp",
"LastUpdatedAt": "timestamp"
},
...
],
"NextToken": "string"
}
```

URI request parameters

- **DomainName**
  
  The unique name of the domain.
  
  - Length Constraints: Minimum length of 1. Maximum length of 64.
  
  - Pattern: ^[a-zA-Z0-9_-]+$
  
  - Required: Yes

- **MaxResults**
  
  The maximum number of objects returned per page.
  
  - Valid Range: Minimum value of 1. Maximum value of 100
• **NextToken**

  The pagination token from the previous ListCalculatedAttributeDefinition API call.
  • Length Constraints: Minimum length of 1. Maximum length of 1024

**GetCalculatedAttributeForProfile**

**GetCalculatedAttributeForProfile**

Initiates the calculation and retrieves the result of a single calculated attribute for a single profile.

**Request**

```
GET /domains/DomainName/profile/ProfileId/calculated-attributes/CalculatedAttributeName
```

**Request Body**

The request does not have a request body.

**Response**

```
{
    "Name": "string",
    "DisplayName": "string",
    "Value": "string",
    "IsDataPartial": "string"
}
```

**URI request parameters**

• **DomainName**

  The unique name of the domain.
  • Length Constraints: Minimum length of 1. Maximum length of 64.
• Pattern: ^[a-zA-Z0-9_-]+$  
• Required: Yes

• **CalculatedAttributeName**
  
The unique (per domain) name of the calculated attribute.
  
• Type: String
  
• Length Constraints: Minimum length of 1. Maximum length of 64.
  
• Pattern: ^[a-zA-Z0-9_-]+$  
• Required: Yes

**ListCalculatedAttributesForProfile**

Initiates the calculation and retrieves the results of all calculated attributes for a single profile.

**Request**

```
GET /domains/DomainName/profile/ProfileId/calculated-attributes?max-results=MaxResults&next-token=NextToken
```

**Request Body**

The request does not have a request body.

**Response**

```json
{
   "Items": [
      {
         "CalculatedAttributeName": "string",
         "DisplayName": "string",
         "Value": "string",
         "IsDataPartial" : "string"
      },
      ...
}
Creating a custom calculated attribute definition

Using the Customer Profiles CreateCalculatedAttributeDefinition API, you can programmatically create your own calculated attribute based on a custom object type.

In this topic we show how to create a calculated attribute using a custom JSON file.

Step 1: Create a JSON file

Create a JSON file with the following contents:
To customize the JSON with your own values, follow these guidelines:

- **Attributes**: This should contain the name of the field from your object type that you want to use for the calculated attribute. Two attributes being referenced in this list are supported.

- **Expression**: Basic math expressions to perform between attributes are supported. If you only have one attribute, this field should be `{ObjectTypeName.AttributeName}`, otherwise if you have a math expression in mind this field should contain both attributes.

- **Statistic**: This is the operation performed when you call one of the calculate APIs that actually performs the aggregation operation. Most are self-explanatory, but we have added explanations for ones that aren’t.

**Supported statistics**

- FIRST_OCCURRENCE returns the attribute specified in the expression of the earliest ingested object.
• LAST_OCCURRENCE returns the attribute specified in the expression of the latest ingested object.
• COUNT returns the count from the selected data.
• SUM returns the sum from the selected data.
• MINIMUM returns minimum from the selected data.
• MAXIMUM returns maximum from the selected data.
• AVERAGE returns average from the selected data.
• MAX_OCCURRENCE returns the most frequently occurring value specified in the expression.

• Range: Currently support DAYS and calculated attributes can be based on up to 366 days of data.

• ObjectCount: Indicates how many objects the calculated attribute calculation should be based on. Values of 1-100 are supported.

• Threshold: If instead of the exact calculated attribute value you instead want to know if it's, for example, greater than a certain value, you can use a threshold.

The threshold value can be any string, and the following threshold operators are supported.

• GREATER_THAN
• LESS_THAN
• EQUAL_TO
• NOT_EQUAL_TO

Step 2: Call the CreateCalculatedAttributeDefinition API

After you have created and customized the JSON file with your values, call the CreateCalculatedAttributeDefinition API, as shown in the following example:

```
aws customer-profiles create-calculated-attribute-definition --cli-input-json file:///custom_calculated_attribute_cli.json --region region_name
```

You can also use the following endpoint:

```
https://profile.your-region.amazonaws.com/domains/your-domain-name/calculated-attributes
```
Validating calculated attribute values using the API

There are two APIs, GetCalculatedAttributeForProfile and ListCalculatedAttributesForProfile, that are at the profile level.

- **GetCalculatedAttributeForProfile** - retrieves a single calculated attribute for a single profile.
- **ListCalculatedAttributesForProfile** - retrieves a list of calculated attributes for a single profile

With a valid profile ID, you should see values for your calculated attributes:

**Example response**

```
{
   "CalculatedAttributeName": "_average_hold_time",
   "DisplayName": "Average hold time",
   "IsDataPartial": "true",
   "Value": "24144"
}
```

**IsDataPartial** - This flag means that either the time range (30 days) or object count have not been achieved and therefore the calculated attribute is still being calculated. For example, if you want an average over 30 days, only after 30 days have elapsed will the IsDataPartial field be set to false.

**Retrieve a list of calculated attributes**

**Use the AWS CLI**

```
aws customer-profiles list-calculated-attributes-for-profile --region your-region --domain-name your-domain-name --profile-id your-profile-id
```

**Use the AWS CLI with a custom JSON file**

Create a JSON file with the following contents:

```
{
   "DomainName": "your-domain-name",
}
"ProfileId" "some-profile-id"
}

aws customer-profiles list-calculated-attributes-for-profile --region your-region --cli-input-json file://list_calculated_attributes_for_profile_cli.json

Endpoint:
https://profile.your-region.amazonaws.com/domains/your-domain-name/profile/your-profile-id/calculated-attributes/

Retrieve a single calculated attribute

Use the AWS CLI:

aws customer-profiles get-calculated-attributes-for-profile --region your-region --domain-name your-domain-name --calculated-attribute-name your-calculated-attribute-name --profile-id your-profile-id

Use the AWS CLI with a custom JSON file:

Create a JSON file with the following contents:

{
  "DomainName": "your-domain-name",
  "CalculatedAttributeName": "your-calculated-attribute-name",
  "ProfileId" "your-profile-id"
}

aws customer-profiles get-calculated-attributes-for-profile --region your-region --cli-input-json file://list_calculated_attributes_for_profile_cli.json

Endpoint:
https://profile.your-region.amazonaws.com/domains/your-domain-name/profile/your-profile-id/calculated-attributes/your-calculated-attribute-name
Default Calculated Attributes

Amazon Connect Customer Profiles provides seven out-of-the box default attributes based on contact records. The attributes are as follows:

New customer

```json
{
    "CalculatedAttributeName": "_new_customer",
    "DisplayName": "New customer",
    "Description": "Returns true or false for new customer profiles created.",
    "CreatedAt": null,
    "LastUpdatedAt": null,
    "Statistic": "TIME_DIFFERENCE_FROM_NOW",
    "Conditions": {
        "ObjectCount": null,
        "Threshold": {
            "Value": "30",
            "Operator": "LESS_THAN"
        }
    },
    "AttributeDetails": {
        "Attributes": [
            {
                "Name": "createdAt"
            }
        ],
        "Expression": "{profile.createdAt}"
    },
    "Tags": {}
}
```

Most frequent channel

```json
{
    "CalculatedAttributeName": "_most_frequent_channel",
    "DisplayName": "Most frequent channel",
    "Description": "Returns customer's frequently used communication channel. Channels include voice, chat, task."
}
```
"CreatedAt": null,  
"LastUpdatedAt": null,  
"Statistic": "MAX_OCCURRENCE",  
"Conditions": {  
  "Range": {  
    "Value": 30,  
    "Unit": "DAYS"  
  },  
  "ObjectCount": null  
},  
"AttributeDetails": {  
  "Attributes": [  
    {  
      "Name": "channel"  
    }  
  ],  
  "Expression": "{CTR.channel}"  
},  
"Tags": { 
} 
} 

Last channel 

{  
  "CalculatedAttributeName": "_last_channel",  
  "DisplayName": "Last channel",  
  "Description": "Returns customer's last communication channel. Channels include voice, chat, task.",  
  "CreatedAt": null,  
  "LastUpdatedAt": null,  
  "Statistic": "LAST_OCCURRENCE",  
  "Conditions": {  
    "ObjectCount": null  
  },  
  "AttributeDetails": {  
    "Attributes": [  
      {  
        "Name": "channel"  
      }  
    ],  
    "Expression": "{CTR.channel}"  
  },  
  "Tags": { 
  } 
}
Last agent identifier

```json
{
    "CalculatedAttributeName": "_last_agent_id",
    "DisplayName": "Last agent identifier",
    "Description": "Returns identifier of the last agent customer connected with.",
    "CreatedAt": null,
    "LastUpdatedAt": null,
    "Statistic": "LAST_OCCURRENCE",
    "Conditions": {
        "ObjectCount": null
    },
    "AttributeDetails": {
        "Attributes": [
            {
                "Name": "agent.id"
            }
        ],
        "Expression": "{CTR.agent.id}"
    },
    "Tags": {
    }
}
```

Frequent caller

```json
{
    "CalculatedAttributeName": "_frequent_caller",
    "DisplayName": "Frequent caller",
    "Description": "Returns true or false based on the number of times a customer has called.",
    "CreatedAt": null,
    "LastUpdatedAt": null,
    "Statistic": "LAST_OCCURRENCE",
    "Conditions": {
        "ObjectCount": null
    },
    "AttributeDetails": {
        "Attributes": [
            {
                "Name": "agent.id"
            }
        ],
        "Expression": "{CTR.agent.id}"
    },
    "Tags": {
    }
}
```
"Statistic": "COUNT",
"Conditions": {
  "Range": {
    "Value": 30,
    "Unit": "DAYS"
  },
  "ObjectCount": null,
  "Threshold": {
    "Value": "5",
    "Operator": "GREATER_THAN"
  }
},
"AttributeDetails": {
  "Attributes": [
    {
      "Name": "contactId"
    }
  ],
  "Expression": "{CTR.contactId}"
},
"Tags": {
}
}

Average hold duration

{
  "CalculatedAttributeName": "_average_hold_time",
  "DisplayName": "Average hold time",
  "Description": "Returns customer's average hold time for voice calls."
}
"Attributes": [
    {
      "Name": "agent.customerHoldDurationMillis"
    },
    {
      "Name": "queue.durationMillis"
    },
    "Expression": "\{CTR.agent.customerHoldDurationMillis\} + \{CTR.queue.durationMillis\}"
],
"Tags": {}
}

Average call duration

{
  "CalculatedAttributeName": "_average_call_duration",
  "DisplayName": "Average call duration",
  "Description": "Returns customer's average call duration for voice calls.",
  "CreatedAt": null,
  "LastUpdatedAt": null,
  "Statistic": "AVERAGE",
  "Conditions": {
    "Range": {
      "Value": 30,
      "Unit": "DAYS"
    },
    "ObjectCount": null
  },
  "AttributeDetails": {
    "Attributes": [
      {
        "Name": "disconnectTimestamp"
      },
      {
        "Name": "initiationTimestamp"
      }
    ],
    "Expression": "\{CTR.disconnectTimestamp\} - \{CTR.initiationTimestamp\}"
}
Error state and troubleshooting

The following table shows calculated attributes error messages, cause, and resolution for each error.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieval of a calculated attribute for a profile shows a null value</td>
<td>This is likely due to the calculated attribute not having data. After creation of a calculated attribute, new data must be ingested.</td>
<td>Ingest new data or re-ingest old data via integrations or the CreateProfile and PutProfileObject APIs.</td>
</tr>
</tbody>
</table>

Amazon Connect admin website

Contents

- How to create Calculated Attributes
- How to view Calculated Attributes
- How to edit Calculated Attributes
- How to delete Calculated Attributes

How to create Calculated Attributes

1. To create calculated attributes, ensure that you have created security profiles permissions as a prerequisite. For more information, see How update permissions for Calculated Attributes.
2. Choose Create attribute in the Calculated attributes table view.
### Calculated attributes
Customer data transformed into actionable data points. Use calculated attributes with flows to personalize customer experiences.
To help you get started, we provided default calculated attributes. [Learn more](#)

#### Attributes (16)
Attributes are calculated for individual profiles, when at least one event occurs within the specified time period.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Time period</th>
<th>Creation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>average call duration</td>
<td>Default</td>
<td>Returns customer’s average call duration for voice calls.</td>
<td>30 days</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>average hold time</td>
<td>Default</td>
<td>Returns customer’s average hold time for voice calls.</td>
<td>30 days</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>frequent caller</td>
<td>Default</td>
<td>Returns true or false based on the number of times a customer has called.</td>
<td>30 days</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>last agent id</td>
<td>Default</td>
<td>Returns identifier of the last agent customer connected with.</td>
<td>-</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>last channel</td>
<td>Default</td>
<td>Returns customer's last communication channel. Channels include voice,...</td>
<td>-</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>most frequent channel</td>
<td>Default</td>
<td>Returns customer's frequently used communication channel. Channels include voice,...</td>
<td>30 days</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>new customer</td>
<td>Default</td>
<td>Returns true or false for new customer profiles created.</td>
<td>-</td>
<td>5/13/2023</td>
</tr>
<tr>
<td>attribute name</td>
<td>Custom</td>
<td>-</td>
<td>1 day</td>
<td>10/23/2023</td>
</tr>
<tr>
<td>household</td>
<td>Custom</td>
<td>-</td>
<td>7 days</td>
<td>10/12/2023</td>
</tr>
<tr>
<td>calculator</td>
<td>Custom</td>
<td>CalclulatorNew</td>
<td>1 day</td>
<td>10/23/2023</td>
</tr>
</tbody>
</table>

3. To create a calculated attribute, assign a name, add the description (optional), and choose the required fields:

- **Calculation**: defines how attributes are computed (average/count/sum/minimum/first occurrence/last occurrence/max occurrence)
- **Attribute**: which is a data point from your customer profiles data
4. Additionally, you can add another attribute by selecting the *plus* icon. You can choose up to two attributes to calculate. When multiple attributes are chosen, they must be combined by an operator. Specify an operator such as *plus* or *minus* to combine the attribute values.
5. Once the calculation is selected, you can select the time period (up to 366 days) and the number of events (up to 100) under the **Event settings**. An output will be returned when there is at least one event during the specified time period.

6. Choose **Create** to create the calculated attribute.

7. Once a calculated attribute has been created successfully, a banner is displayed on the table view with a link to add a flow for a calculated attribute.
How to view Calculated Attributes

1. Login to Amazon Connect admin website with your credentials. Once logged in choose Calculated Attributes from the Customer Profiles menu in the left navigation panel.

2. Choose an item on the Name field in the table view to view details of the attribute.
3. You will now be able to view the details of the attribute that you had selected.

How to edit Calculated Attributes

1. To edit a calculated attribute, choose an attribute in the table view by selecting the radio button, which enables the **Edit** button. Choose **Edit**.
2. You will be able to edit the **Description**, **Time period**, and **Number of events**. Once edited choose **Save**.

### Calculated attributes
Customer data transformed into actionable data points. Use calculated attributes with flows to personalize customer experiences.
To help you get started, we provide default calculated attributes. [Learn More](#)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Time period</th>
<th>Creation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>average_call_duration</td>
<td>Default</td>
<td>Returns customer's average call duration for voice calls.</td>
<td>30 days</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>average_hold_time</td>
<td>Default</td>
<td>Returns customer's average hold time for voice calls.</td>
<td>30 days</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>frequent_caller</td>
<td>Default</td>
<td>Returns true or false based on the number of times a customer has called.</td>
<td>30 days</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>last_agent_id</td>
<td>Default</td>
<td>Returns identifier of the last agent customer connected with.</td>
<td>-</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>last_channel</td>
<td>Default</td>
<td>Returns customer's last communication channel. Channels include voice,...</td>
<td>-</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>most_frequent_channel</td>
<td>Default</td>
<td>Returns customer's frequently-used communication channel. Channels i...</td>
<td>30 days</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>new_customer</td>
<td>Default</td>
<td>Returns true or false for new customer profiles created.</td>
<td>-</td>
<td>5/15/2023</td>
</tr>
<tr>
<td>attribute_time</td>
<td>Custom</td>
<td>-</td>
<td>1 day</td>
<td>10/25/2023</td>
</tr>
<tr>
<td>average_customer_service_time</td>
<td>Custom</td>
<td>-</td>
<td>2 days</td>
<td>11/15/2023</td>
</tr>
<tr>
<td>Average-Order-Price-Per-Week</td>
<td>Custom</td>
<td>Average Order price per week for a customer</td>
<td>7 days</td>
<td>11/15/2023</td>
</tr>
</tbody>
</table>

How to edit Calculated Attributes
How to delete Calculated Attributes

1. To delete a calculated attribute, choose an attribute in the table by selecting the radio button next to the attribute that you would like to delete.

2. Once selected, choose **Delete**.

3. In the **Delete Attribute** pop-up, verify the details and enter *confirm* to enable the **Delete** button.

4. Choose **Delete**.

Use the Customer Profiles API

For information about how to programmatically manage domains and profiles, see the Amazon Connect Customer Profiles API Reference.

We recommend using the CustomerProfileJS open source library when integrating Customer Profiles into your own agent application. For more information, see the CustomerProfilesJS repo on Github.

For more information about how to integrate your existing apps with Amazon Connect use Amazon Connect Streams. You can embed the Contact Control Panel (CCP) components into your app.
Example: Programmatically integrate S3 with Customer Profiles

Using the Customer Profiles PutIntegration API, you can programmatically create integrations for S3, Salesforce, Marketo, and more.

In this topic we show how to create an S3 integration with a sync interval of 15 minutes, the minimum value currently supported.

Step 1: Create a JSON file

Create a JSON file with the following contents:

```json
{
    "DomainName": "your-domain",
    "ObjectTypeName": "your-object-name",
    "FlowDefinition": {
        "FlowName": "your-flow-name",
        "KmsArn": "the key ARN is the same as your domain's key",
        "Description": "Created by Customer Profiles",
        "TriggerConfig": {
            "TriggerType": "Scheduled",
            "TriggerProperties": {
                "Scheduled": {
                    "ScheduleExpression": "rate(15min)",
                    "DataPullMode": "Incremental",
                    "ScheduleStartTime": 1634244800.435,
                    "FirstExecutionFrom": 1594166400
                }
            }
        },
        "SourceFlowConfig": {
            "ConnectorType": "S3",
            "SourceConnectorProperties": {
                "S3": {
                    "BucketName": "your-bucket",
                    "BucketPrefix": "your-prefix"
                }
            }
        },
        "Tasks": [
            {"TaskType": "Filter", "SourceFields": ["colA", "colB"], "ConnectorOperator": {"S3": "PROJECTION"}}
        ]
    }
}
```
To customize the JSON with your own values, follow these guidelines:

- **FlowName**: Can be STRING [a-zA-Z0-9][\w!@#.-]+
- **ScheduleStartTime**: Set to the current DateTime + 5 minutes in epoch time.
- **FirstExecutionFrom**: Go to S3, look at the file date, and use a date that is before the oldest date.
- **Tasks**: Define TaskType. In the Sourcefields field you have to supply ALL the columns you have in your CSV in that array. Then, for each of the items in that array, you need to specify the ConnectorOperator. This example is for a CSV document with two columns: colA and colB.

### Step 2: Call the PutIntegration API

After you have created and customized the JSON file with your values, call the **PutIntegration** API, as shown in the following example:

```bash
aws customer-profiles put-integration --cli-input-json file:///put_integration_s3_cli.json --region us-west-2
```

The response from PutIntegration returns a flow URI. For example:

```json
{
   "DomainName": "testDomain",
   "ObjectType": "your objec type",
   "CreatedAt": "2021-10-14T13:51:57.748000-07:00",
   "LastUpdated": "2021-10-14T13:51:57.748000-07:00",
   "Tags": {}  }
```
Step 3: Call the Amazon AppFlow StartFlow API

Use the flow URI to call the Amazon AppFlow StartFlow API. For example:

```
aws appflow start-flow --flow-name uri --region us-west-2
```
Forecasting, capacity planning, and scheduling

To run a contact center, you need the right number of agents working at the right times to achieve your operational goals. It’s critical to not overspend or overrun your workforce.

Amazon Connect provides a set of services powered by machine learning that help you optimize your contact center by offering the following:

- **Forecasting.** Analyze and predict contact volume based on historical data. What will future demand—the contact volume and handle time—look like? Amazon Connect forecasting provides accurate and auto-generated forecasts that are automatically updated daily.

- **Scheduling.** Generate agent schedules for day-to-day workloads that are flexible, and meet business and compliance requirements. Offer agents flexible schedules and work-life balance. How many agents are needed in each shift? Which agent works in which slot?

- **Schedule Adherence.** Enable contact center supervisors to monitor schedule adherence and improve agent productivity. Schedule adherence metrics are available after the agent schedules are published.

- **Capacity planning.** Predict how many agents your contact center will require. Optimize plans by scenarios, service level goals, and metrics, such as shrinkage.

For information about where Amazon Connect forecasting, capacity planning, and scheduling is available, see [Availability of Amazon Connect services by Region](#).

The following diagram shows a typical end-to-end optimization workflow by persona: Amazon Connect administrator, forecaster, scheduler, capacity planner, and agent. It lists the tasks performed by each persona.
Get started with forecasting, capacity planning, and scheduling

Use these steps to set up forecasting, capacity planning, and scheduling.

1. **Enable forecasting, capacity planning, and scheduling** in the Amazon Connect console.

   **Note**
   After enabling Forecasting, capacity planning, and scheduling, it may take up to **24 hours** before the feature is available for use.

2. **Assign security profile permissions** to the Amazon Connect users who will use this feature.

Use the following steps to start using forecasting, capacity planning, and scheduling.

1. **Set the forecast and scheduling interval**
2. **Create forecast groups**
3. **Create forecasts**
4. **Create capacity planning scenarios**
5. **Create staff rules**

Enable forecasting, capacity planning, and scheduling

You must enable forecasting, capacity planning, and scheduling at the Amazon Connect instance level. After you enable forecasting, capacity planning, and scheduling, it may take up to 24 hours for the feature to be available for use in your AWS account.

1. Log in to the [AWS Management Console](https://aws.amazon.com) using your AWS account.

2. In the AWS Management Console, at the top of the page in the search bar, type *Amazon Connect* and then choose *Amazon Connect*. This is shown in the following image.
3. On the Amazon Connect virtual contact center instances page, choose the Instance alias where you want to enable forecasting, capacity planning, and scheduling.

4. In the navigation pane, choose Forecasting, capacity planning, and scheduling.
5. On the **Forecasting, capacity planning, and scheduling** page, select the check box to enable forecasting, capacity planning, and scheduling.

6. The status changes to *In progress*, as shown in the following image.
7. Within 24 hours the status will change to *Enabled* and forecasting, capacity planning, and scheduling will be ready to use.

Security profile permissions for forecasting, capacity planning, and scheduling

Assign the following security profile permissions as needed to use forecasting, capacity planning, and scheduling:
• **Approve**: Users with the Approve permission will be able to view, create, edit, and approve time off requests.

• **Capacity planning**: This permission allows you to view and edit in capacity planning pages, including scenario and capacity plans. It also allows users to import future estimated shrinkage and available FTEs.

• **Forecasting**: This permission allows you to view and edit in forecasting pages. For example, you can create, view, publish, and delete forecast groups and forecasts, import historical data from external applications, and more.

• **Individual schedule calendar**: This permission allows agents to view their schedule in their agent application.

• **Schedule manager**: This permission allows you to view and edit generated schedules from the schedule manager. The view permission also enables you to view historical schedule adherence metrics. (Note: You still need the View Metrics Permission in addition to this permission)

• **Team schedule calendar**: After a schedule is published, this permission enables you to view or edit the published schedule. You can see the schedule calendar, but agents cannot. The view permission also enables you to view historical schedule adherence metrics.

> **Note**

You still need the View Metrics permission in addition to this permission.

• **View**: Users with the View permission will be able to view time off requests in the Time off Requests drawer. Users with the View permission will not be able to create or approve time off requests.

For information about how to add more permissions to an existing security profile, see [Update security profiles](#).

By default, the **Admin** security profile already has permissions to perform all forecasting, capacity planning, and scheduling activities.

**Troubleshooting forecasting, capacity planning, and scheduling**

These sections outline troubleshooting scenarios and address frequently asked questions for forecasting, capacity planning, and scheduling.

• **Forecasting**
• **Capacity planning**

• **Scheduling**

**Forecasting**

• **How can I create an ad hoc forecast?**

Forecasts are processed automatically, delivering short-term forecasts daily, and long-term forecasts weekly, so users don’t need to worry about running forecasts manually. However, you may want to see how a forecast is updated when you add or modify historical data. For example, if you had an anomaly in your historical contact volume, and you don’t want the machine-learning model to use that anomaly in building a forecast, you can modify the historical data and then when the new forecasts are run, the new forecasts will not incorporate that data.

To see the most recent forecasts, check the **Last computed** column.

New forecasts will be generated when a user uploads or deletes historical data using the **Import data** tab or adds/removes queues from a forecast group.

![Table](image)

**• When I import historical data it returns errors.**

Select **download details** to ensure that the imported data is in the correct format: If there are any errors, check the error details. It will provide additional details for the specific error. You must ensure that your file is in .csv format, contains no decimals, no extra rows, or column fields. For more information on the required format, see [Import historical data for forecasting](#).
• Forecast failed due to error: Insufficient data in Amazon Connect.

When you receive this error, it could be due to three different reasons:

1. You have less than 6 month of historical data. To address this problem, upload more historical data. While Amazon Connect can generate forecasts with six months of data, we recommend at least 12 months of recent contact data to ensure that contact patterns (for example, seasonality) are properly captured. If you don’t have 6 months of data, you can give Connect synthetic (artificial) data that will be used to generate the forecast. Alternately, you can upload your own forecast using the Override function.

2. You need at least 2,000 contacts per month across all of your forecast groups. Amazon Connect generates forecasts using historical data for all queues that are included across all forecast groups. At least 2,000 monthly contacts in the past 6 months for the Amazon Connect instance are required to successfully generate a forecast. Amazon Connect does not require 2,000 monthly contacts for every queue. All queues in all forecast groups must total more than 2,000 monthly contacts.

3. You need recent data. Amazon Connect performs a data recency check (is the data recent enough) based on the aggregation of all queues included across all forecast groups. At least one data point in the past four weeks is required to successfully generate a forecast.

• Cannot import data, cannot download forecast, cannot create forecast group, or cannot create forecast.

Most likely, you do not have the correct permissions. Check with your admin to ensure you have permissions for Analytics, Forecasting - Edit.

• Forecasting override upload failed.

Check the error message to make sure the .csv file format matches our data schema. For more information on the required format, see Import historical data for forecasting.

Tip

download the computed or published forecast .csv file. Take the time period for override, and copy the queue ID and queue name, time stamps to the override template.
Note, only the latest uploaded .csv file will be used, and the previous uploaded files will be overridden.

- **Long-term Forecast failed even after I have uploaded more than 6 months of data.**

  The data uploads for long-term and short-term forecasts are independent, so you will need to upload these separately: one for long-term and one for short-term. First, check if you also uploaded the daily historical data for long-term forecast. The 15 to 30 minute interval data is for short-term forecasts only. Second, check if the long-term daily level .csv file has more than 6 consecutive months historical data counted from now.

- **Short-term forecast failed even after I uploaded more than 6 month of data.**

  The data uploads for long-term and short-term forecasts are independent. The daily interval data is for long-term forecast only. First, check if you uploaded the 15 or 30 minute interval historical data for short-term forecast and the file has more than 6 consecutive month data. Second, check what is the forecast interval setting in .csv file to ensure it matches the historical intervals on the UI.

- **Why am I unable to publish a forecast?**

  It's possible that you do not have permissions to publish a forecast. It's also possible that the forecasts (both contact volume and handle time for each of short-term and long-term) have not been successfully generated. Check if you have the permission for **Analytics, Forecasting - Publish** and check if the forecasts have been successfully generated (the status column should show *complete*" when the forecasts are generated).

- **How can I see data from a previous period?**

  You are able to view forecasts in a specified period that occurred in the past.
Can I see past forecast data?

You can see the last published and the last computed forecast. The last computed forecast will be overwritten once the next forecast is computed. If you wish to retain this data, you can download the `.csv` file that contains the last computed and published forecasts.

Why are the forecasts used in capacity planning different than the ones I see in forecasting or scheduling?

The forecast that is used in capacity planning is the most recent published long-term forecast. You may see a different forecast in forecasting if you are looking at the most recent computed forecast in comparison to a published forecast. You will see a different forecast in scheduling, as that is the most recently published short-term forecast.

Why do I see the call volume peak in short-term forecast at mid-night when no traffic is expected?

Forecasting uses Coordinated Universal Time (UTC) as its time zone. For North American users on the Pacific or Atlantic Coasts, this is 8 hours ahead of PST, or 7 hours ahead of PDT; and 5 hours
ahead of EST, or 4 hours ahead of EDT. So for example, midnight in UTC is 4pm PST / 5pm PDT or 7pm EST / 8pm EDT.

Note

It’s important to remember to use UTC time when uploading historical data or overrides.

- Why am I unable to delete a forecast?

Forecasts can only be deleted if they are not being used for a capacity plan (long-term forecast) or schedule (short-term forecast). Check if the forecast has been published and that it is used for scheduling or capacity planning. You must delete the schedule or capacity plans in order to delete the forecast.

- Why do the long-term and short-term forecasts show different values for the same time period?

These two forecasts have different training frequencies and different models, as they are optimized for different purposes. Short-term is designed for interval level granularity over a period of weeks and long-term is designed for daily granularity over a period of months.

- Why is long-term average handle time flat but short-term average handle time isn’t?

A flat average handle time performs better when forecasting short-term forecast workloads as it displays interval granularity over a period of weeks. Allowing the average handle time to vary in a long-term forecast results in better performance as displays daily granularity over a period of months.

Handle time is important when calculating a workload. It generally doesn’t vary much in the short term but can vary over longer time periods, which is reflected in our models.

- Is call volume counted at the time when the call comes in, or when the call ends?

Call volume starts counting at the time when call comes in. For example, a call started at 4:50 PM, and ends at 5:05 PM. It will be counted as the call volume for the 4:45 PM - 5:00 PM interval.

Capacity planning

- How do I handle shrinkage in capacity planning?
Users can increase capacity planning accuracy by providing estimated future data, which includes available full-time employees (FTE) and Shrinkage, for the existing forecast groups. Providing Available FTE and shrinkage data is optional. Amazon Connect can generate a capacity plan without it but providing it improves the accuracy of the capacity plan. In order to import that data, download the .csv template from the UI and fill out the empty cells. Note that users need to enter the exact name of the forecast groups they created. Also, users can add multiple forecast groups in this .csv file. For more information, see Import estimated future shrinkage and available full-time employees.

- **I am seeing errors during data import in capacity planning.**

Confirm that the forecast group names in the .csv file match the actual forecast group names in forecasting module.

**Scheduling**

- **The system does not generate schedules for some or all of my agents. What should I check?**

This can occur due to the fact that the last date an agent can be scheduled is before the time of the schedule and/or the agent's maximum working hours don't allow them to work in that shift profile. Review the following steps to address this issue.

1. Check **Staff Rules** to ensure that the **End date** is not configured for agents who do not have a schedule. **End date** allows schedulers to specify the last date that an agent can be scheduled until.

2. Check shift profiles to see if the **Start time** and **End time** hourly schedule window is equal to or more than **Maximum working hours** per agent. For example, if the shift profile is configured to generate a schedule of an 8 hour duration, when the agent's staff rule is configured for them to work 4 hours per day, the system will apply the staff rule and only generate a schedule for 4 hours.

- **Why am I unable to access the scheduling page while on my company's VPN?**

It is possible that your company's VPN has security measure in place that could be preventing access to the needed endpoints. If you are unable to access the scheduling page while connected to your company's VPN, reach out to your admin or network security team to have them allowlist the following endpoints:
• Why are lunch activities for some agents scheduled before the first break activity, even though I have specified a lunch activity to be placed after the break?

This can be caused by having overlaps in the break and lunch activities. Check the specific shift profile to see if the placement window for both activities overlap. For example, you may have configured a break activity to be placed between 11am and 1pm and a lunch activity to be placed between 10am and 3pm, so the system may choose to place the break at 12:30pm and the lunch at 11:30am. Remove or minimize the overlap of activity placement windows to solve this issue.

• Why do I see agents get scheduled at different start times than expected?

This is commonly caused by challenges with time zones. Shift profiles are set using Coordinated Universal Time (UTC), and staff rules specify which time zone agents should use. Review the following steps to address this issue.

- Ensure the **shift profile** start time and end time are configured in the UTC time-zone.
- Ensure the correct user time-zones are set in the **Staff rules** UI. For example, if you want to schedule agents in Boston (EST time-zone) from 9am to 5pm, you must do the following.
  - Set **Shift profile** start time as 1:00pm and end time as 9pm. Usually shift profiles are set once and later re-used.
  - Updated the timezone for all agents to EST time zone in the **Staff rules** UI.

• Can I view the schedule in my local time?

Yes. Supervisors and schedulers can view schedules in their local time zone for agents they manage. Agents can view their individual schedules in their local time zone. User time zones can be set in the **Staff rules** UI.

• Do I need to define activities for workloads like phone or chat?

No. **Work** will be the default activity on the schedule if there is no break or lunch scheduled for the time slot. Only define the activities for the agent when they are not taking a call or responding to a chat.

• Why did some agents did not get added to the roster for certain days?
How agents are added to the roster depends on multiple configurations in staffing groups and staff rules, such as min/max working hours, min staff required, or min/max consecutive work days. The service will take the defined working hours and add an agent to the roster by taking into consideration other rules that have been defined in staffing groups and staff rules. For example, if the minimum working hours are 40 hours, and the agent belongs to a staff group that operates 12 hours per day and 6 days per week, then the agent is likely to have some days without schedules. The service optimizes schedules based on forecasts. As long as the minimum amount of 40 hours per week (4 days with 10 hours per day) is met, the agent may not be staffed on some days when the call volume is low. In cases where you see that an agent doesn’t have a schedule for a day, check the agent’s minimum working hours. Also, check if the agent has been added to the roster for the remainder of the week.

- Why is my agent's scheduled time different than the shift profile time? For example, my shift profile has 10 hours every weekday, but my agent only gets scheduled for 6 hours?

The shift profile operation hours apply to staffing groups. If you don’t set the staffing groups rule for shift start time, the service will optimize your agent start time based on the forecasted workload. For example, the shift profile has 8 AM - 6 PM Monday - Friday, and the workload is light in the morning, and heavier in the afternoon. Each agent has a minimum of 6 hours and a maximum of 8 hours per day. To save agent cost, the service will schedule less agents in the morning and more agents in the afternoon. Some agents could start at 8 AM, some could start at 8:30 AM, and some could start in the afternoon. Some agents could have 6 hour schedules and some could have 8 hour schedules. In this way, you can maximize your agent resources to meet the service goal. If you want every agent to start at the same time and work an exact number of hours, you can set the rule in the staffing group shift start time to start at the same time and set the working hour to 10 hours every day. In this case, savings on agent cost will be less due to less flexibility to optimize based on forecasts.

### Rules:

<table>
<thead>
<tr>
<th></th>
<th>Min. hours</th>
<th>minutes</th>
<th>Max. hours</th>
<th>minutes</th>
<th>Per period</th>
<th>Week</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Time</td>
<td>40</td>
<td>0</td>
<td>50</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Working hours should also include total time spent on non productive activities like breaks.

<table>
<thead>
<tr>
<th></th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Staff Required</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shift Start Time</td>
<td>Same Start Time</td>
</tr>
</tbody>
</table>
• My agents are all full-time employees and they work 8 hours per day. How can I set this up in my schedule?

Set your staffing group's and staff's maximum and minimum working hours to 8 hours a day.

• I have a mix of full-time and temporary employees. What is the best way to define it?

The best practice is to use staffing groups to set the working hours to the 8 hours and then use staff rules to set the individual part-time agent working hours to their specific value. The value in the staff rule will override the value in the staffing group.

• How do I add meetings or one-off events?

Generate a schedule with daily activities first. In the schedule manager view, select any schedule, and use add shift to add a one-off shift activity to the schedule.

Forecasting in Amazon Connect

Forecasting is the starting point for any scheduling and capacity planning activities. Before you can generate a schedule or capacity plan, you must create a corresponding forecast.

A forecast attempts to predict future contact volume and average handle time. We use historical metrics to create the forecast.

Short term forecasts are automatically updated every day. When you come into work, you can review the forecast that was updated overnight with the most current data. You can publish the forecast to make it available to schedulers whenever you want. The Forecasting page displays when a forecast was last updated and published. Use published short term forecasts for scheduling.

Long term forecasts are automatically updated every week, based on the day you created the forecast. For example, if you created the forecast on a Monday, it is updated every Monday. Use published long term forecasts for capacity planning.
Important

Only the most current forecast is available. Because the forecast is updated every day, if you want to keep the current day's forecast, you must download it before Amazon Connect overwrites it.

Getting started with forecasting

Use the following steps to create a forecast and then share it with other people in your organization.

1. Set the forecast and scheduling interval: This is a one-time activity typically set up by forecasters. It cannot be undone.
2. Create forecast groups
3. Import historical data
4. Create forecasts
5. Inspect a forecast
6. Publish a forecast

There are other things you can do with a forecast, such as download to a .csv file for offline analysis or override it, but these steps will get you started.
Set the forecast and schedule interval

You can set the granularity for your short-term forecasts and your schedules.

Important things to know

- You must have security profile permissions for **Analytics, Forecast and schedule interval - Edit**. For more information, see **Assign permissions**.
- You must specify an interval for short-term forecasting and scheduling.
- Amazon Connect supports 15- or 30-minute intervals. For example, if you select 30 minutes as the interval, your short-term forecasts are generated for 30-minute intervals (that is, 20 contacts between 9:00 AM-9:30 AM), and your schedules are computed for 30 minute intervals.
- You must set up a forecast and a schedule interval before you can generate forecasts or create forecast groups.
- After you set the forecast and schedule interval, you cannot change it.

To set the forecast and schedule interval

1. Log in to the Amazon Connect admin website.
2. On the Amazon Connect navigation menu, select **Analytics and optimization, Forecasting**.
3. Choose the **Forecast and schedule interval** tab. You'll see this tab only if you have the appropriate security profile permissions.

```
Forecasts        Forecast groups      Import data   Forecast and schedule interval

Forecast and schedule interval

Forecast and schedule granularity is measured at either 15 or 30 minutes. Once set, you will not be able to change this. Learn more

15 minute interval
30 minute interval

Save   Cancel
```

4. Choose one of the following options:

- **15 minute interval** – Generates short-term forecasts in 15-minute intervals. For example, 20 contacts between 9:00 AM to 9:15 AM, and 30 contacts between 9:15 AM to 9:30 AM.
• **30 minute interval** – Generates short-term forecasts in 30-minute intervals. For example, 20 contacts between 9:00 AM to 9:30 AM, 30 contacts between 9:30 AM to 10:00 AM.

**Create forecast groups**

Forecast groups are a way for you to combine different queues into one forecast. This enables you to create a forecast from aggregated data from multiple queues, instead of from just one queue.

**Important things to know**

- Forecast groups are associated with a staffing group for scheduling purposes. Therefore, we recommend you group queues that share the same pool of staff (agents) under the same forecast group. It enables you to generate a more accurate forecast.
- Each queue can belong to only one forecast group. This prevents duplicates in the forecast.
- You must create at least one forecast group before you can generate any forecast.
- We strongly recommend that you create all forecast groups before creating any forecast.

Amazon Connect uses historical data for queues included in all forecast groups to train your forecasting model. By creating forecasts after all forecast groups are created, you ensure historical data of all relevant queues are included in the training.

- If a queue is associated with a forecast group and is later disabled, you don't have to remove this queue from the forecast group. This is because: Although the queue is included by the forecast group and the historical data associated with it is included in the forecast, over time, no contact reaches the disabled queue, and thus stops impacting the forecast. Only the active queues contribute to the forecast.

**How to create forecast groups**

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Forecasting - Edit**.

   For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Forecasting**.

3. Select the **Forecast groups** tab, and then choose **Create forecast group**.
4. On the **Create Forecast Groups** page, under **Queues**, you'll see a list of queues that are not yet associated with a forecast group are listed. If no queues are listed, it means they are all associated with a forecast group already.

5. Drag and drop one or more queues to the forecast group, as shown in the following image. You can press and hold CTRL (COMMAND for macOS users) or SHIFT to select multiple queues at a time.

![Create Forecast Groups](image)

6. Choose **Save**. The following image shows the new forecasting group, along with the number of queues in the group and the date it was last changed.

![Forecasting](image)

7. After creating a forecast group, you can add or remove queues. However, doing so might initiate an immediate change in associated forecasts.

For example, if you made a change for forecast group today, Amazon Connect automatically computes the new short-term and long-term forecasts tomorrow. Your change to the forecast group also impacts downstream capacity plans and schedules that are created based on the forecast group.
The following image shows a sample warning message when adding a queue may trigger an immediate change in associated forecasts. You must choose **Confirm** if you want to continue.

8. You can remove the forecast group by using the **Remove** function.
   
a. delete the forecasts that are associated with the forecast group you want to delete.

   For example, in the following image, a forecast group named *Network_Issues* cannot be deleted because this forecast group was used to create forecasts.

   Therefore, go to **Forecasts** tab to delete those associated forecasts.

   b. Delete the forecast group.

**Next steps**

Now you're ready to create a forecast. For instructions, see **Create forecasts**.

**Import historical data for forecasting**

Amazon Connect requires sufficient historical data to learn the contact pattern and make good forecasts. By default, it uses historical contact data in Amazon Connect for forecasting. You can
import historical data from external applications for Amazon Connect to use for forecasting. When you import data, Amazon Connect uses both its data and the imported data for forecasting. However, the imported data takes precedence over the Amazon Connect data.

**When to import data**

We recommend importing historical data from external applications in the following use cases:

- **Insufficient historical data in Amazon Connect.** If you have less than one year of historical data in Amazon Connect, we strongly recommend that you extract historical data from your previous system and upload the data to Amazon Connect. It is fine to have data split between your Amazon Connect data and uploaded historical data. For example, if you want to generate forecasts on January 1, 2022, and you have nine months of historical in Amazon Connect (from April 1 to December 31, 2021), we recommend importing three additional months of data (from January 1 to March 31, 2022) to make a continuous one-year historical data set available.

  **Important**
  
  If you have less than six months of recent historical data in Amazon Connect, the forecast will fail. You must import additional historical data to unblock forecasting. For more information, see [Data requirements for forecasting](#).

- **Incorrect historical data in Amazon Connect.** If the historical contact pattern is incorrect (for example, the contact volume is abnormally low on the day of a wide-spread power outage in the contact center), you can import data that is more representative to override historical data and correct for the anomaly.

If you have more than one year of historical data in Amazon Connect, you can choose to skip data import and start creating forecasts.

**Important things to know**

- The data file must be a .csv file and it must be in the required format. If the file format and data don't meet the requirements, the upload does not work. We recommend downloading and using the template provided through the Amazon Connect admin website (see step 4 in [How to import historical data](#)) to help you prepare the historical data.

  The following image shows an example of the .csv template. There are headings in the first row for QueueName, QueueId, ChannelType, and so on.
Following are the requirements for imported data:

- **QueueName**: Enter the Amazon Connect queue name.
- **QueueId**: Enter the Amazon Connect queue ID. To find the queue ID in the Amazon Connect admin website, on the left navigation, go to **Routing, Queues**, choose the queue, select **Show additional queue information**. The queue ID is the last number after /queue/.
- **ChannelType**: Enter **CHAT** or **VOICE**. You must capitalize the channel type.
- **TimeStamp**: Enter the timestamp in UTC (ISO8601) format, with a letter Z (the abbreviation of Zulu Time - Coordinated Universal Time) at the end.
- **IntervalDuration**: Enter **15mins** or **30mins** for short-term forecast, depending on your forecast and schedule interval. Enter **daily** for long-term forecast.
- **IncomingContactVolume**: Enter the number of inbound, transfer, and callback contacts as an integer.
- **AverageHandleTime**: Enter the amount of average handle time (in seconds) as type double/decimal.
- **ContactsHandled**: Enter the number of inbound, transfer, and callback contacts handled as an integer.

You can import multiple files. You do not have to consolidate all data in one big file. You can divide data by year, queue, interval duration types, and more, per your preference.

If duplicate data are found across multiple files, the last uploaded records are used. For example:

1. You have the original historical data (from Amazon Connect) from 7/1 to 8/1.
2. You uploaded a new historical data file X to override 7/10 to 8/1.
3. You uploaded another new historical file Y to override 7/15 to 8/1.
4. And now, the historical data baseline is: 7/1 to 7/9 from original, 7/10 to 7/14 from file X, 7/15 to 8/1 from file Y.

- You need to upload historical data *separately* for short-term and long-term forecast.
- Data aggregated in 15- or 30-minute intervals is used for short-term forecasting.
- Data aggregated at daily grain is used for long-term forecasting.
For example, if you only upload data in 15- or 30-minute interval, you won't be able to generate long-term forecasts.

- The following special characters are allowed in the .csv file: -, _, ., (, and ). Space is allowed.

The following image shows an example of what the data looks like in a CSV file that has been opened with Excel.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Column header</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QueueName</td>
<td>QueueId</td>
<td>ChannelType</td>
<td>TimeStamp</td>
<td>Interval</td>
<td>IncomingVolume</td>
<td>AverageHandleTime</td>
<td>ContactsHandled</td>
</tr>
<tr>
<td>2</td>
<td>Accepted value/format</td>
<td>Queue name in Connect</td>
<td>36-digit queue_id in Connect</td>
<td>- VOICE</td>
<td>UTC (ISO8601)</td>
<td>- 15mins, - 30mins, daily</td>
<td>Integer</td>
<td>Integer</td>
</tr>
<tr>
<td>3</td>
<td>Notes</td>
<td>QueueId is available in Connect UI. (Click 'show additional info in queue page')</td>
<td>Has to be capitalized</td>
<td>Has to be one of the three values above</td>
<td>The number of incoming, outbound, and callback contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Example: a record in a file uploaded for short-term forecast.</td>
<td>Queue1</td>
<td>gbsey48s-5222-50ac-6217-353881aaf95e</td>
<td>CHAT</td>
<td>2020-02-14T05:00Z</td>
<td>15mins</td>
<td>20</td>
<td>250</td>
</tr>
<tr>
<td>5</td>
<td>Example: a record in a file uploaded for long-term forecast.</td>
<td>Queue1</td>
<td>gbsey48s-5222-50ac-6217-353881aaf95e</td>
<td>VOICE</td>
<td>2020-02-14T00:00Z</td>
<td>daily</td>
<td>150</td>
<td>200</td>
</tr>
</tbody>
</table>

How to import historical data

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Analytics, Forecasting - Edit.

For more information, see Assign permissions.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Forecasting, and then choose the Import Data tab.

3. Choose Upload data.

4. On the Upload historical data dialog box, choose download the CSV template for historical data.

5. Add historical data to the .csv file, and then choose Upload file to upload it. Choose Apply.

6. If the upload fails, choose download details to view the error log message for more information. The following image of the Forecasts page shows the location of the download details link, next to the Failed status message.
The following image shows the download details file opened by using Notepad. It indicates the error is in Row 2, the QueueId is not valid.

7. If the forecast was uploaded successfully, its **Status** = **Complete** and **Date uploaded** = today.

Delete imported historical data

You can delete previously imported historical data in Amazon Connect. Note that the historical data deletion or addition will trigger an immediate change in associated forecasts because this action will change the historical data baseline that the model is trained for. The following image shows an example warning message about the consequences of removing data.

After the imported historical data is deleted, the last previously uploaded data is used for the baseline. Take the previous example:

- You have the original historical data (from Amazon Connect) from 7/1 to 8/1.
- You uploaded a new historical data file X to override 7/10 to 8/1.
- You uploaded another new historical file Y to override 7/15 to 8/1.
- And now, the historical data baseline is: 7/1 to 7/9 from original, 7/10 to 7/14 from file X, 7/15 to 8/1 from file Y.
- If:
  1. You deleted file Y, the baseline will be: 7/1 to 7/9 from original, 7/10 to 8/1 from X.
  2. You deleted file X, the baseline will be: 7/1 to 7/14 from original, 7/15 to 8/1 is from Y.
Data requirements for forecasting

Amazon Connect generates forecasts using a machine-learning model tailored for contact center operations. It requires a sufficient amount of recent contact data to ensure the model is trained with relevant data and is able to generate high-quality forecasts.

Important things to know

• Amazon Connect generates forecasts using historical data for all queues included in all forecast groups.

• Amazon Connect performs a data sufficiency check (is there enough data) based on the aggregation of all queues included in all forecast groups.
  • At least 2,000 monthly contacts in the past six months are required to successfully generate a forecast.
  • Amazon Connect does not require 2,000 monthly contacts for every queue. At least one forecast group should have more than 2,000 contacts per month for the last 6 months.

• While Amazon Connect can generate forecasts with six months of data, we recommend 12 months of recent contact data to ensure contact patterns (for example, seasonality) are properly captured.

• Amazon Connect performs a data recency check (is the data recent enough) based on the aggregation of all queues included in all forecast groups.
  • At least one data point in the past four weeks is required to successfully generate a forecast.

Do I have a sufficient amount of recent contact data?

• If you have been using Amazon Connect for more than 12 months, you do not need to provide any additional data.

• If you have been using Amazon Connect for more than six months but less than 12, we recommend providing additional historical data. You can import historical data from a source that is external to Amazon Connect. For instructions, see Import historical data.

• If you have been using Amazon Connect for less than six months, make sure it has at least six months of data. Otherwise, forecasting will fail.

For instructions about how to import more data, see Import historical data.
Create forecasts

Forecasts are a projection of the workload in your contact center. Amazon Connect provides long-term and short-term forecasts for you to generate capacity plans and agent schedules. The forecasts include inbound, transfer, and callback contacts in both voice and chat channels.

After creating a forecast, you will not need to generate it manually.

- Short-term forecasts are scheduled to run automatically every day.
- Long-term forecasts are automatically updated every week, based on the day you created the forecast. For example, if you created the forecast on a Monday, it is updated every Monday.
- Every forecast is computed using the most current contact data.
- The models for short-term and long-term forecasts are retrained on a weekly and monthly basis respectively to incorporate the latest contact pattern.
- You can delete forecasts. Downstream capacity plans and schedules created based on the forecasts will be impacted.

To create a forecast

1. Before creating a forecast, you must create at least one forecast group. If you haven't yet done that, see Create forecast groups. We strongly recommend creating all of your forecast groups before creating any forecast.

2. Log in to the Amazon Connect admin website with an account that has security profile permissions for Analytics, Forecasting - Edit.

   For more information, see Assign permissions.

3. On the Amazon Connect navigation menu, select Analytics and optimization, Forecasting.

4. Select the Forecast tab, and then choose Create Forecast.

5. On the Create Forecast page, choose the forecast groups.
6. Choose the forecast type. Amazon Connect creates a forecast for each type you select.

- **Long term** forecasts are used for capacity planning. For example, how many Full Time Equivalent (FTE) agents you need to hire in the next few months, quarter, and year.

- **Short term** forecasts are used for scheduling agents and interval level agent headcount estimation.

7. Choose **Save**. If the forecast group has already been included in a forecast, an error message is displayed.

8. If the forecast was created successfully, it's Status = **Scheduled**.

   The status is **Complete** when the computation finishes. You can use **Search** to find forecasts by forecast group name.

9. Amazon Connect creates a forecast for each forecast type, as shown in the following image.

   ![Forecast Group](image)

   **Inspect a forecast**

   You can inspect your forecasts before publishing them. You can do this in the online Amazon Connect admin website, or **download the forecasts** for offline analysis.
To help make it easier to inspect a forecast in the Amazon Connect admin website, the forecast data is displayed in both a graph and a table. Use the controls on the report settings panel and calendar picker to adjust and filter the data for a more granular view. For example, you can:

- Use the calendar to change the horizon. You can zoom into specific dates.
- Choose 15 minute intervals if your date range is less than a week. This enables you to see the exact contact pattern of the day.
- Compare Last computed forecast and Last published forecast as shown in the following image.
- Compare Actuals and forecasts to identify any abnormalities in either the line chart or the "Variance" chart. The following image shows the forecast data is displayed as graphs.

Choose the Override setting to inspect the effect of any override you uploaded. The Override option is active only after an override has been uploaded. For more information, see Override a forecast.

- Filter by queues or channels to limit your forecast to one or more type.

**Download a forecast**

You can download a forecast so you can inspect it offline. A forecast is downloaded as a .csv file of the forecast data. It has the queue name, channel type, timestamp, incoming contact volume and average handle time data.
1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Forecasting - Edit**.

   For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, choose **Analytics and optimization, Forecasting**.

3. On the **Forecasts** tab, choose the forecast.

4. Choose **Actions**, and then download either the last computed forecast or the last published forecast.

5. We recommend choosing **click here**. This enables you to choose the name of the file download and where to save it, as shown in the following image. Otherwise, the file is saved to your **Downloads** folder and its name is a generated number.

![Forecast for: Widget Support](image)

---

**Override a forecast**

You can override the forecast at the queue channel level by uploading a .csv file. Override allows you to modify forecasts and make sure the forecasts reflect the contact pattern in special events (for example, a one-off marketing event that can increase volume by 10 percent in a given week).

You can also remove the override if the override is no longer applicable.
Important things to know

• To override a forecast, you need to prepare and upload a .csv file with your override data. Currently Amazon Connect does not support changing the values in forecasting user interface directly.

• The override data file be must a .csv file and it must be in the required format. If the file format and data don't meet the requirements, the upload does not work. We recommend downloading and using the template provided to help you prepare the historical data.

The following image shows an example csv file with data in it.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column header</td>
<td>QueueName</td>
<td>QueueId</td>
<td>ChannelType</td>
<td>TimeStamp</td>
<td>IntervalDuration</td>
<td>AverageHandleTime</td>
<td>IncomingContactVolume</td>
</tr>
<tr>
<td>1</td>
<td>Accepted value/format</td>
<td>Queue name in Connect</td>
<td>36-digit queue_id in Connect</td>
<td>- VOICE - CHAT</td>
<td>UTC (ISO8601)</td>
<td>- 15mins - 30mins - daily</td>
<td>Integer</td>
</tr>
<tr>
<td>3</td>
<td>Notes</td>
<td>QueueId is available in Connect UI (Click &quot;show additional info&quot; in queue page)</td>
<td>Has to be capitalized</td>
<td>Has to be one of the three values above</td>
<td>Average handle time (AHT) for contacts</td>
<td>The number of incoming inbound, transfer, and callback contacts</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Example</td>
<td>Queue1</td>
<td>abseiy48u-1522-51ca-86f7-86f7</td>
<td>CHAT</td>
<td>2020-02-14T00:00Z</td>
<td>15mins</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Queue1</td>
<td>abseiy48u-1522-51ca-86f7</td>
<td>VOICE</td>
<td>2020-02-14T00:00Z</td>
<td>daily</td>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>

Following are the requirements for imported data:

• QueueName: Enter the Amazon Connect queue name.

• QueueId: Enter the Amazon Connect queue ID. To find the queue ID in the Amazon Connect admin website, on the left navigation, go to Routing, Queues, choose the queue, select Show additional queue information. The queue ID is the last number after /queue/.

• ChannelType: Enter CHAT or VOICE.

• TimeStamp: Enter the timestamp in UTC (ISO8601) format.

• IntervalDuration: Enter 15mins or 30mins for short-term forecast, depending on your forecast and schedule interval. Enter daily for long-term forecast.

• IncomingContactVolume: Enter the number of inbound, transfer, and callback contacts as an integer.

• AverageHandleTime: Enter the amount of average handle time (in seconds) as type double/decimal.

• You can upload only one override file for a forecast group.

• This means if you previously uploaded an override file (for example, with 120 lines of overrides), you must add new overrides to this override file (for example, add 50 new lines of overrides) and re-upload the file that now has 170 lines of overrides.
• This also means you will need to include overrides for both short-term and long-term forecasts in one file.

• Both contact volume and Average Handle Time metrics are included in one override file. Both columns must be populated in the override file.

• The following special characters are allowed in the .csv file: -, _, ., (, and ). Space is allowed.

**How to override a forecast**

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Forecasting - Edit**. For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Forecasting**, and then choose the **Forecast** tab.

3. Choose the forecast.

4. Choose **Actions, Upload forecast override**.

5. Choose **Download the CSV template for override data**.

   ![Note]

   Amazon Connect supports one, which would be the latest, override file per forecast group.

   • If you have never uploaded an override file, your template will contain headings but no data.
   • If you have uploaded override file in the past, your template will be the previously uploaded file.

   If you need to make changes later on to the same forecast, you must download the last uploaded file, make your changes, and then upload the file. Amazon Connect retains only the last uploaded file.

6. Add override data, and then choose **Upload file** to upload it. Choose **Apply** to confirm forecast override.
## Publish a forecast

When you publish a forecast, you make it visible to other users, such as capacity planners and schedulers, so that they can use the forecasts for capacity planning and scheduling.

⚠️ **Important**

Amazon Connect retains only the last published forecast. We strongly advise you to download the last published forecast before publishing a new one because the last forecast will be permanently replaced. For instructions, see [Download last published forecast](#).

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Forecasting - View**.

   For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Forecasting**.

3. On the **Forecasts** tab, choose the forecast.

4. Choose **Actions, Publish forecast**.

5. Choose the forecasts.

   The status is **Complete** for successfully published forecasts. When publish fails, the status is **Publish failed**.

### Download the last published forecast

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Forecasting - View**.

   For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Forecasting**.

3. On the **Forecasts** tab, choose the forecast.

4. Choose **Actions, Download last published forecast**.

5. We recommend choosing **click here** as shown in the following image. This enables you to specify the name of the downloaded file and the location. Otherwise, the file is saved to your **Downloads** folder and its name is a generated number.
Capacity planning in Amazon Connect

A capacity plan helps you estimate the long-term FTE (full-time equivalent) requirements for your contact center, up to 18 months. It specifies how many FTE agents are required to meet the service level target for a certain period of time.

After you generate long term FTE estimations, you can share this information with other stakeholders, such as Human Resources, Finance, and the Training Department, to help facilitate the hiring and training of staff. When a business launches a new product or extends into a new Region, staff hiring is needed to meet the customer service demand.

The capacity planning feature uses published long-term forecasts as input, along with scenario information that you provide. It then creates a long-term capacity plan that you can share with stakeholders. The following diagram illustrates this integration among published long-term forecasts, capacity planning, and capacity planning output.
Following is the order of steps for creating a capacity plan and sharing it with others.

1. **Create capacity planning scenarios**

2. **Import estimated future shrinkage and available full-time employees**: This is an optional step but it can improve the accuracy of your capacity plan.

3. **Create capacity plans using forecasts and scenarios**

4. **Create capacity planning scenarios**

5. **Review, override, re-run, or download** a capacity plan.

6. **Publish a capacity plan**

### Create capacity planning scenarios

A scenario has two parts:

- **Scenario inputs**: The maximum occupancy, daily attrition, FTE hours per week. For example, you might enter data that represent your best case scenarios (everyone is at work) or worst case scenarios (a large number of people are out sick during winter months).

- **Optimization inputs**: The service level or average speed of answer (ASA). For example, 85% of calls are answered within 30 seconds of entering the queue.

You can then use this scenario to generate a capacity plan that represents how many people you need to hire accordingly to meet your business goals. The output includes the required FTE employees with and without shrinkage, forecasted occupancy rate, the gap between available required FTEs, and maximum overtime (OT) and voluntary time-off (VTO) rate allowed.

### To create a capacity planning scenario

1. **Before you can create a capacity plan, you must create and publish a long-term forecast.** Amazon Connect uses the published long-term forecast as the input for creating the capacity plan. If you haven't yet created a forecast, see [Getting started with forecasting](#).

2. **Log in to the Amazon Connect admin website with an account that has security profile permissions for Analytics, Capacity planning - Edit.**

   For more information, see [Assign permissions](#).
3. On the Amazon Connect navigation menu, choose **Analytics and optimization, Capacity planning**.

4. On the **Planning Scenarios** tab, choose **Create a Scenario**.

5. On the **Create scenario** page, enter a name and description.

6. In the **Scenario inputs** section, enter the following information:

   a. **Max Occupancy (optional)**: The percentage of time agents will spend handling contact volume when they log in.

      i. **Daily attrition**: The percentage of staff leaving your contact center.

         For example, if the annual attrition is 50%, the daily attrition would be $\frac{50\%}{250}$ working days per year = 0.2%.

      ii. **Full-time equivalent (FTE) hours per week**: How many hours each FTE employee will work per week.

   b. **Outsourced contacts (optional)**: You can outsource a percentage to a third-party.

   c. **Max overtime (OT) allowed (optional)**: Specify the maximum percent of overtime to plan for peaks. As a planner, you don’t want to burn out your workforce.

      For example, you specify 40 as FTE hours per week, with 10 percent maximum overtime. The total work week would be up to 44 hours.

   d. **Max voluntary time off (VTO) allowed (optional)**: Specify the maximum percent of time off to plan for troughs, when there is a lull in contacts and you can save in costs. Be sure not to give too much time off in case traffic increases again.

      For example, you specify 40 as FTE hours per week, with 10 percent maximum time off. The total work week would be at least 36 hours.

7. In the **Optimization inputs** section, enter the operational goals for your organization:

   a. **Service level**: The percentage of contacts answered within a defined target time threshold.

      The following image shows service level targets where 80 percent of voice contacts and 70 percent of chat contacts will be answered within 30 seconds.
b. **Average speed of answer (ASA):** The average amount of time it takes for contacts to be answered in a call center during a specific time period.

c. You can create one goal per channel. Choose **Add another goal** to add another goal.

### Import estimated future shrinkage and available full-time employees

You can increase capacity planning accuracy by providing estimated future data (Available FTE and Shrinkage) for your existing forecast groups. Providing Available FTE and shrinkage data is optional. Amazon Connect can generate a capacity plan without it, but providing it improves the accuracy of your plan.

#### How to import data

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Capacity planning - Edit**.

   For more information, see **Assign permissions**.

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Capacity Planning**.

3. On the **Import Data** tab, choose **Upload data**.

   The .csv file you upload must have the following headings: FORECAST_GROUP, Date, AVAILABLE_FTE, IN_OFFICE_SHRINKAGE_OUT_OFFICE_SHRINKAGE. These are shown in the following image of a CSV file opened with Excel.
Update values in this template, and then choose Upload CSV to upload it. Choose Upload.

It usually between 2 - 5 minutes for the .csv file to upload. If the upload fails, check if the FORECAST_GROUP name in the .csv file matches the name of the forecast group that you created.

**Important things to know about your .csv file**

- **FORECAST_GROUP**: Enter the EXACT name of the forecast group you created. You can add multiple forecast groups in this .csv file.
- **Date**: Each row is one day. In the previous image, row 2 is January 1, row 3 is January 2, row 4 is January 3, and so on. Use ISO 8601 format ending with Z.
- **AVAILABLE_FTE**: Based on your estimation, how many full-time agents will be available for working that day. For example, your contact center currently has 100 FTEs and you expect this number to be the same next year.

In the previous image, 0 indicates no full-time agents are available on January 1 for the forecast group named **Forecast For Demo**. On January 3, 100 agents are available.

**Tip**

Required FTE (the output) is how many full-time agents are required to meet the Service Level target. For example, if the Required FTE = 120 and Available FTE = 100 for next year, then that means a deficit = 20.

- **IN_OFFICE_SHRINKAGE**: Percentage of agents in the office but not in production mode. For example, they might be in training or in meetings.
- **OUT_OFFICE_SHRINKAGE**: Percentage of agents absent from work (for example, no show or personal time off).
**Note**

The latest uploaded .csv file always overrides the previous one you updated. Make sure errors aren't introduced to the uploaded .csv file accidentally. For example, don't press Enter and add new rows to the end of the file. Otherwise, the data won't validate and an error message is displayed.

---

**Create capacity plans using forecasts and scenarios**

Before you can create a capacity plan, you must create a planning scenario and publish a long-term forecast. Amazon Connect uses the forecasts and planning scenarios as inputs for creating the capacity plan. If you haven't yet created a forecast and planning scenario, see [Getting started with forecasting](#) and [Create capacity planning scenarios](#).

**How to create a capacity plan**

1. Navigate to the **Capacity Plans** tab, and choose **Generate Plan**.

2. Provide the plan name, description, forecast group (which has published long-term forecasts), start/end date, and plan scenario. The following image shows example values for these fields.
3. Choose **Generate Capacity Plan**.

4. To quickly identify the plan that is in processing, choose **Last Computed** to sort the table list. In the following image, the status of the plan is **In Progress**.

It usually takes between 5-10 minutes for the plan to be generated. If the plan generation fails, try publishing the selected long-term forecasts, and then generating the capacity plan again.
Review capacity plan output

To review capacity plan output, choose the hyperlink for the plan you generated. The first half of the page summarizes the input you used in scenario and capacity plan generation.

The plan output shows a week-by-week or month-by-month calculation. To switch from weekly to monthly view, select Monthly from the dropdown, as shown in the following image.

Following is a description of the metrics in the plan output:

• **Forecasting Inputs**
  - **Forecasted Contact Volume**: This metric is a sum of both voice and chat volume for the selected forecast group.
  - **Forecasted Average Handling Time (AHT), seconds**: This metric shows the aggregated AHT for the selected forecast group.
  - The forecasted contact volume and AHT in the plan output table reflects only the values from the selected forecast group. After there are newly published forecasts, consider re-running the capacity plan to reflect the latest published contact volume and AHT.

• **Outputs**
  - **Required FTEs (without Shrinkage)**: How many full-time equivalent agents need to be hired to meet the defined business goals (such as service level target), without considering shrinkage.
  - **Forecasted Occupancy %**: How much occupancy is for the agents.
• Outputs with additional input
  • Required FTEs (with Shrinkage): How many full-time equivalent agents needed to be hired to meet the defined business goals (such as service level target), with considering shrinkage.
  • Available FTEs: How many agents are available for working that day. It can be uploaded in the Import data section.

• Metrics calculated from available FTE input
  • Gap between available FTEs and required FTEs: The difference between available FTEs and required FTEs.
  • Gap %: The percentage of the gap.
  • Required OT %: if there is a supply deficit (required FTEs higher than available FTEs), required OT% indicates how much overtime would be needed to cover the deficit.
  • Required OT %: If there is a supply surplus (the number of required FTEs is lower than the available FTEs), required VTO % indicates how much voluntary time off could be used to lower the amount of agent idle time and thus lower costs.

Override a capacity plan

You can upload a .csv file that overrides the Required FTEs (without Shrinkage) data in the Plan outputs section of a capacity plan. This section is shown in the following image.

You might want to do this, for example, to give your team of agents a buffer.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Analytics, Capacity planning - Edit.
For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Capacity Planning.

3. On the Capacity Plans tab, choose the plan.

4. On the detailed page for the capacity plan, choose Actions, Upload plan override, and then choose download the CSV template file. This option is shown in the following image.

The .csv file template has one row, and it contains the values that were displayed in the Required FTEs (without Shrinkage) row of the Plan outputs table. The following image shows an example of this data in a .csv file

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Metrics</td>
<td>Jan 6 - Jan 12, 2022</td>
<td>Jan 13 - Jan 19, 2022</td>
<td>Jan 20 - Jan 26, Jan 27 - Feb</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Required FTEs (without Shrinkage)</td>
<td>79</td>
<td>78</td>
<td>81</td>
<td>78</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Make your changes, and save the template file with a different name. Return to the Upload override dialog box (you might need to choose Actions, Upload plan override to redisplay the dialog box), choose Upload CSV, and then choose Override.

6. After you upload the .csv file, the metrics in the Required FTEs (without Shrinkage) row are automatically re-calculated and updated. Hover over the blue triangle to see the original value, as shown in the following image.
7. The rest of the metrics are updated automatically to reflect the latest change for Required FTEs (without Shrinkage).

**Re-run a capacity plan**

You can re-run capacity plans when you make any changes on the plan start and/or end date, or the scenario. When there are no changes to plan inputs or the scenario, the **Re-run plan** option is not active, as shown in the following image.

![Plan Outputs](image)

- **To re-run a plan**
  1. Go to the **Capacity Plans** tab, and choose the plan.
  2. Change the start and/or end date, or select a different scenario.
  3. Choose **Actions, Re-run plan**.
Download a capacity plan

When you download a capacity plan file, it downloads as a .csv file type with multiple tabs. It's helpful to open this file using Excel. The following image shows an example of what a capacity plan file looks like in Excel. It has the following worksheets: Metrics, Capacity Plan, Scenario, Generation Details.

Following is a description of each worksheet:

- **Metrics**: The capacity plan output.
- **Capacity Plan**: The capacity plan metadata, such as name, starting date, and ending date of the plan.
- **Scenario**: The input defined for the capacity plan.
- **Generation Details**: The metadata indicating when someone last changed the capacity plan.
How to download capacity plan results

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Analytics, Capacity planning - Edit**.
   
   For more information, see [Security profile permissions for forecasting, capacity planning, and scheduling](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Capacity Planning**.

3. On the **Capacity Plans** tab, choose the plan.

4. On the detailed page for the capacity plan, choose **Actions, Download capacity plan**.

Publish a capacity plan

When you are satisfied with the capacity plan outputs, choose **Publish plan** to finalize your plan.

⚠️ **Note**

You cannot edit the plan after it is published.

Your login name and the published date is displayed on the list view of the capacity plans. For example, the following image shows a plan that was first created on January 11, 2022, and then it was published on January 20, 2022 by Admin.

![Capacity Plan Details](image)

Scheduling in Amazon Connect

Contact center schedulers or managers need to create agent schedules for day-to-day workloads that are flexible and meet business and compliance requirements. Amazon Connect helps you create efficient schedules that are optimized for per-channel Service Level or Average speed of answer targets. You can generate and manage agent schedules based on the following:

- A short-term published forecast
• Shift profiles (templates for weekly shifts)
• Staffing groups (agents that can handle specific types of contacts from a specific forecast group)
• Human resources and business rules

Note
Amazon Connect scheduling is not designed to ensure compliance with any particular laws. It is your responsibility to ensure that your actions and your use of scheduling comply with any applicable laws including employment regulations. You should confer with your legal counsel to determine your obligations.

Getting started

Following is the order of steps for creating a schedule and publishing it so supervisors and agents can view it.

1. Add users to your Amazon Connect instance.
2. Double-check with your Amazon Connect admin that users have the required security profile permissions to access scheduling features. The required permissions are described here.
3. Create staff rules for scheduling
4. Create shift activities
5. Create shift profiles
6. Create staffing groups and rules
7. Generate, review, and publish a schedule by using Schedule Manager

To learn how supervisors and agents view schedules, see How supervisors view published schedules and How agents view their schedule.

Scheduling roles: Who does what

There are a variety of roles for people who might create and manage schedules in a contact center, such as the following:

1. Amazon Connect administrator – Maintains user profiles, grants security profile permissions, sets up holiday hours for the contact center.
2. **Scheduler** – Creates manages staffing groups, creates staffing rules, configures shift components (such as creating shift activities and profiles), generates schedules, revises, and publishes schedules.

   After the scheduler publishes a schedule, the supervisors and agents receive a notification in the user interface that the schedule has been published and they can view it.

3. **Supervisor** – Manages agents and schedules, updates schedules, manages requests for time off, overtime (OT), and voluntary time off (VTO).

4. **Agent** – Answers contacts, views the generated schedule, manages requests for time off, overtime (OT), and voluntary time off (VTO).

Amazon Connect provides security profile permissions that you can assign to each role, so that you can manage access to specific features by role. For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

### Scheduling terminology

**Draft schedule**

A collection of schedules for all agents in a set of staffing groups that the schedule is for.

Only schedulers can view and adjust draft schedules. Agents or their supervisors cannot view these schedules until published.

**Overtime / Time off / Voluntary time off**

- Requesting overtime to agents allows your contact center to handle a contact surge or agent shortages without hiring more employees.
- Requesting time off to agents allows your business to handle contacts while paying employees.
- Requesting voluntary time off to agents allows your business to handle contacts without paying employees to be idle.

**Publish a schedule**

An action taken by schedulers to make agent schedules formal and visible in agent and supervisor Schedule calendars (which are separate user interfaces).
Schedule

Multiple shifts tied together between the start and end dates for a specific agent.

Schedule adjustment

Before schedule publishing to supervisors or agents, the Scheduler or the person with permission can add, edit, remove, replace agent activities, or edit and remove shifts to orchestrate supply (that is, the number of agents and shift activities) vs demand (the number of contacts).

Schedule generation

The ability to generate and publish shift schedules for specific date range for a Forecast Group - Staff Group combination.

Shift activities

Daily activities that the agent does during their shift. For example, meetings, training, and lunch.

Shift profiles

The base structure of a shift, schedule window, daily shift activities that go into it.

Staffing groups

A group or team of agents who are skilled to take specific types of contacts. For example, you might create one staffing group named General Enquiry, and another named Tier 2 Support.

Create staff rules for scheduling

Use staff rules to specify optional details for individual agents and supervisors, such as their local time zone, start and end dates, and contract details.

- The individual staff rules you specify here override any staffing group rules when their schedule is generated.

For example, you might set up the staffing group to generate a schedule where everyone works 40 hours per week. In the staff rules, you can choose specific employees to schedule for 20 hours per week.
Create staff rules for individuals

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Scheduling, Schedule manager - Edit.

For more information, see Assign permissions.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Scheduling.

3. On the Scheduling page, choose the Staff Rules tab, and then search and choose one or more staff from the list. Every time a staff is selected, the staff count is displayed in the Apply to Staff button.

4. Specify optional details such as:

   • Time zone: Render schedules in the local time zone of the agent.
   • Shift start and end dates: Schedule specific agent shifts based on start or end dates.
   • Working hours and minutes: Define the minimum and maximum working hours per day and per week. Working hours should include non-productive time, such as breaks and meals.

For example:

   • If you want to generate agent schedules that are 8 hours and 30 minutes long each day, then specify 8 hours and 30 minutes in both min and max working hour fields.
   • If you want to allow the system to generate more efficient schedules, you may provide a min and max working hours window. The system will generate the most optimal schedule duration based on forecasts and agent availability.

   • Consecutive days worked or days off: Schedule shifts based on the allowed range of consecutive days worked or days off.

   • Associate to shift profile: You can assign a shift profile to individual agents. This is useful to do when, for example, you have part-time agents who are in the same staffing group as your full-time agents, but they require their own shift profile.

The following image shows the location of the Associate to shift profile dropdown menu on the Staff rules tab.
5. Choose **Apply to Staff**. This saves the rules, and ensures they are applied during the next scheduling cycle.

**Import time off balance for individuals**

For the maximum file size that you can upload, see *File size per upload of agent time off data* in *Forecasting, capacity planning, and scheduling feature specifications*.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Scheduling, Schedule manager - Edit**.

   For more information, see [Assign permissions](#).

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Scheduling**.

3. On the **Scheduling** page, choose the **Staff Rules** tab.

4. Choose Download template and store the .csv file on your desktop. It looks similar to the following image.

5. Add data or make changes to the .csv file as needed and then save to your desktop with a new file name.

6. Choose **Upload data** to upload the .csv file. Amazon Connect does the following:
• Validates the data and provides details if there are errors.
• Prompts you for confirmation that you want to upload the data.
• Uploads the file and displays a confirmation message when complete.

After the .csv file is successfully uploaded, Amazon Connect checks the available time off balance when time off requests are submitted. If there is enough time off balance it approves the request. Otherwise, the request is declined.

• The time off balance for the requested time off type must be equal to or greater than the duration of the requested time off.

Create shift activities

Shift activities are daily activities that the staff (agents) does during their shift. For example:

• **Productive**: At work activities that agents do that are counted as productive work, such as answering contacts.

• **Non-Productive**: At work activities that agents do that are not counted as productive work, such as breaks and team meetings.

• **Time off**: Absent from work. Their status in the agent application is **Offline**.

You can create multiple shift activities to include as part of your staff shifts.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Scheduling, Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Scheduling**.

3. On the **Scheduling** page, choose the **Shift Activities** tab, and then choose **Add shift activities**. Fill in the details and choose **Save**.

   You can add multiple activities, and add and remove activities.

4. The next time a schedule is created as part of the scheduling cycle, the shift activities are applied.
Tip

Create shift profiles to ensure the desired sequence of the shift activities. For example, to schedule agents to go on their break two hours before lunch. For instructions, see Create shift profiles.

Shift activity descriptions

- **Activity name**: Name of the activity
- **Description (Optional)**: Additional information on the activity
- **Sub-type**
  - **If non-productive: Break or meal**: Set this subtype for breaks, lunches or meal activities. This option is only available for Non-Productive activity types. This setting allows automated break or meal time adjustments when time offs or overtimes are added or removed from staff shifts, to comply with the break rules configured in the Staffing Group and Shift Profiles.
  - **Time off: Staff Requestable**: Setting this option to **Yes** will allow agents to see and pick the respective time off activity during time off creation. Set this option to **No** for time off activities that can only be requested by supervisors on behalf of an agent.
- **Hours and minutes**: Default duration
- **Adherence**: Yes/No
- **Paid**: Yes/No
Create shift profiles

Use shift profiles to create templates for weekly shifts. The template includes the days of the week worked, the earliest start time and the latest end times the staff can be scheduled, the activities they would do during their shift, and various roles.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Scheduling, Schedule manager - Edit.
   
   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Scheduling.

3. Choose the Shift Profiles tab, and then choose Add shift profiles.

4. In the Schedule Window section, complete the section as follows:

   • For Work status, choose one of the following options:

     • Working: This means when Amazon Connect generates the schedule, it must schedule the staff to work between the specified hours and minutes.

     • Flex: This means if Amazon Connect predicts enough contact volume to warrant scheduling the agent, it may schedule them to work between the specified hours and minutes.

   The following image shows the Schedule Window section of the Add shift profile page.
• **Start Time** and **End Time**: Specify the earliest start time and the latest end time for each day. Ensure that these times are configured in UTC instead of local time.

• **Shift length (Optional)**: Specify the maximum shift length that an agent can be scheduled on a specific day. This option is especially useful if your contact center is open for long periods of time, such as 24 hours, but each shift is shorter than that, such as 8 hours.

Depending on the contact demand pattern forecast, Amazon Connect determines the best possible start and end times for shifts, while adhering to the minimum and maximum hours per day and week worked.

5. Choose **Add shift activities**. Select the shift activities the staff will do during their shift. (You create the shift activities that appear in the list, such as Productive, Time off, and Non-Productive.)

6. For each activity, set placement rules. The rules include:

   • The time duration from the beginning to end of the shift where the activities need to be placed.
   • The time window for Amazon Connect to pick the best spot to maximize efficiency of the generated schedules to meet the goals, such as the service level percent (SL%) targets.
7. Optionally, complete the **Rules** section as follows:

⚠️ **Important**

These rules override the settings in the **Schedule Window** section.

Choose the **Add rule** dropdown box and choose from the following options:

- **Minimum break distance**
- **Maximum break distance**
- **Days worked**: If you list multiple days, they are separated by OR.
- **Days off**: If you list multiple days, they are separated by OR.

8. In the **Daily shift activities** section, complete the **Default shift activity group** section to specify when activities such as lunch breaks and training should be scheduled during the shift. The shift activities apply to everyone in the shift. In the following image, agents are scheduled for a **Break** 6 hours after starting their shift and within 7 hours.
Optionally, choose **Add new group** to add a subgroup of agents and specify shift activities for them. In the following image, the shift is 2 hours and no activities are specified. This means the agents in **Shift activity group 2** don't get a break.

9. After saving the shift profile, you can edit or remove it from the list view.

For example, if you set break to start 6 hours after the start of a shift and lunch to start 3 hours after the start of a shift, the lunch is scheduled to occur first.

**Create staffing groups and rules**

A **staffing group** is a group or team of agents who are skilled to take specific types of contacts. You add agents who need a schedule generated for them, and supervisors who manage agent schedules. You can also add rules that apply at the staffing group level, such as the minimum staff required and the minimum working hours per day or week for the group. If a user needs to view published agent schedules from the **Published** calendar view, then the user must be added as a supervisor within the specific staffing group.
For example, say your contact center opens at 9AM but the forecast says no contacts arrive between 9-9:30AM. You can add a rule that says, despite what the forecast predicts, there should be a minimum of one agent during this time.

If you don't have a shift start time rule, then the schedule is built using the predictions from the forecast.

For a list of staffing group limits, see Forecasting, capacity planning, and scheduling feature specifications.

Example

For example, you might create one staffing group named General Enquiry, and another named Tier 2 Support. Because you map one or more staffing groups to a forecast group, here's how you would create staffing groups in this case:

1. Group all General Enquiry queues to a General Enquiry forecast group.
2. Map the General Enquiry forecast group to multiple staffing groups that have agents who can take general enquiry contacts.

Create group and add staff

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Scheduling, Schedule manager - Edit.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Scheduling.

3. Choose the Staffing Groups tab, and then choose Create staffing group.

4. On the Create Staffing Group page, under Associate to forecast group, use the dropdown to choose the forecast group to associate with this staffing group.

   In the following example, contacts from the queues in the Forecast_Group_20220124 will be routed to the agents in this staffing group.

5. Choose Add staff to add agents and supervisors to this staffing group. Only names for Amazon Connect users appear in the list of staff. The following image shows the name Jane Doe, which can be added to the agent list.
Tip

Every agent must be in a staffing group in order for a schedule to be generated for them. You can add and remove agents in between schedule cycles and manually add shifts.

Even after an agent is in a staffing group, you can assign them their own shift profile by using the Staff rules tab. The agent-level shift profile overrides the profile set at the staffing group level. For more information, see Create staff rules for scheduling.

Add rules

To generate a schedule, Amazon Connect uses information from the forecast group, which reflects the historical demand pattern for your contact center. Staffing rules enable you to specify conditions that must be accounted for in the schedule, regardless of what the forecast predicts.

For example, your contact center opens at 9AM but the forecast says no contacts arrive between 9AM-9:30AM. You can add a rule that, despite what the forecast predicts based on historical demand, there should be a minimum of one agent during this time. This forces Amazon Connect to keep one agent in the schedule from 9-9:30AM. In addition, you can add a rule to set the Working Hours to start at 9AM, even though the forecast would start it at 9:30AM.

To add rules

- In the Rules section, choose + and then use the dropdown to choose the type of rule to create for the staffing group. For example, you can specify:
• **Minimum Staff Required**: Specify the minimum number of agents that should be available, despite what the forecast indicates. For example, if the forecast says that you do not need any agents in the first half hour that your contact center opens, you can ensure that there is a minimum of one agent during this time.

• **Shift Start Time: Same Start Time**: This creates schedules with the same shift start time for all agents.

• **Working Hours**: Specify the group's minimum and maximum working hours per day or week. This setting applies to all staff in the staffing group. You can override this setting for individual staff. For instructions, see Create staff rules for scheduling.

**Generate, review, and publish a schedule by using Schedule Manager**

Amazon Connect is designed to generate the least number of shifts for agents based on the forecasted demand pattern and configured constraints to hit the optimization goal.

After you create shift activities, shift profiles, staffing groups and staffing group rules, you can generate a schedule.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for **Scheduling, Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling.

2. On the Amazon Connect navigation menu, select **Analytics and optimization, Scheduling**.

3. Choose the **Schedule Manager** tab, and then choose **Generate schedule**.

4. Enter a name and description for the schedule.

5. In the **Schedule input** section, select the forecast group from the dropdown menu.

   Currently you cannot schedule for multiple forecast groups.

6. Specify the duration of the schedule - the start and end dates. You can schedule up to 18 weeks out.

7. Under **Optimize schedule for**, choose **Service level** or **Average speed of answer**.

8. Average speed of answer (ASA) is an alternative to using service level percentage targets. For example, the following image shows an ASA set to 30 seconds. The capacity planning and scheduling system will optimize headcount / schedules to ensure that the goal is met.
9. Choose **Generate schedule**.

**Note**
Amazon Connect generates a draft schedule. It will not be visible to agents or supervisors until you publish it.

10. In the list of schedules, the schedule you created shows a status of **In progress**. It takes 5-30 minutes to generate, depending on the number of agents, number of configured rules, schedule duration, and more. After the schedule is generated, it's status is **Complete** or **Failed**.

11. To view any warnings, breaches of rules, or constraints breaches, choose the warnings icon, as shown in the following image. More information about the warnings is displayed.
12. When the status is **Complete**, choose the draft schedule to view it. The following image shows a sample schedule for one day, for 10 agents.
Schedulers can:

- View schedules for all agents.
- Pick a date to view a specific shift.
- Navigate back to today's date.
- View failed rules and goals.

13. When you're satisfied with the schedule, choose **Publish**. You'll get a confirmation page. Choose **Proceed** to make the schedule official!

Staff (agents) and supervisors specified in the staffing groups can now view the schedule. See the following topics to learn about their experience:

- [How supervisors view published schedules](#)
- [How agents view their schedule](#)

### Edit a schedule

Before publishing a schedule, you might want to edit it. For example, if you notice that all the agents are scheduled to be on break at the same time and no one is scheduled to take contacts.

You can:

- Change agent shift start and/or end time, duration.
- Change activity shift start and/or end time, duration.
- Add an activity to one or more agents shift.
• Remove or replace activity from an agent shift.
• Copy an entire shift from one agent to another.
• Recompute metrics to ensure schedule adjustments result in better service level (SL%) or occupancy.

The following image shows these options in the dropdown list: **Edit, Add, Replace, Remove, Copy.**

![Schedule options dropdown](image)

**Regenerate a schedule**

Managers and supervisors can regenerate agent schedules for up to six different forecast groups after making changes to the scheduling configuration.

1. To edit a schedule, select the schedule, choose **Actions**, and select **Edit Schedules**. Make your changes and choose **Save**.

2. To regenerate one or more schedules, select the schedules you want to regenerate, choose **Actions**, and select **Regenerate schedules**.

**Search and sort a schedule**

Managers and supervisors can search and sort schedules from within the schedule manager. Schedulers can search for schedule names using partial keywords or sort the schedule list based on start date, end date, creation date, or updated date.

The following image shows the search box on the **Scheduling** page. Entering **mar** returns schedules that have March in their name.
How supervisors view published schedules

After a scheduler publishes a schedule, it's official. Agents can now view their individual scheduling using their agent application. Supervisors can also view their agents schedules using the Amazon Connect admin website.

Supervisors with **Scheduling, Schedule manager - Edit** permissions in their security profile can edit agent schedules.

⚠️ **Important**

When a supervisor edits an agent schedule and publishes it, the change appears immediately to the agent. They do not need to refresh their browser for the agent application to reflect the change.

The following image shows a sample schedule for a supervisor's team.
Managers and supervisors can sort or filter schedules based on the following criteria.

- **Sort** schedules based on the earliest shift start time. For example, the agents who would login first to take customer contacts will show up on top. The following example displays a manager or supervisor who searches for agents by first name, last name, or login ID with the string sa1, sorted by their shift start times.
Filter schedules based on agent names or agent IDs, Staffing Groups, or Supervisor names.
How agents view their schedule

There are two ways agents can access their schedules:

- If your organization uses the Amazon Connect agent application, agents access their schedule by entering `https://instance name/connect/agent-app-v2/` into their browser and then choosing the calendar icon.

- If your organization uses the Contact Control Panel (CCPv1 or CCPv2), Salesforce CTI, or a custom-built agent desktop, agents access their schedule by entering `https://instance name/connect/agent-app-v2/scheduling` into their browser, logging into Amazon Connect, and then choosing the calendar icon.

Following are steps agents use to view their schedule in the agent application.

1. Log on to the agent application using the URL that your admin gives you.
2. Choose the Calendar icon on the application navigation bar to launch the staff schedule manager viewer. Otherwise, the staff schedule manager viewer launches automatically.

The following image shows a sample schedule in the agent application.
You can see a daily or weekly view of your schedule.

**Add shift activities in draft or published schedules**

Amazon Connect scheduling allows contact center managers, supervisors, and schedulers to insert activities into agent schedules, both draft and published. For example, activities such as team meetings, 1:1 coaching sessions, and trainings can be added into an agent's schedule.

**Add a shift activity**

1. Choose the agents you wish to include in the activity by selecting the check-boxes next to their names.
2. Choose the **Actions** drop-down and select **Add Shift Activity**. This action will bring up the **Add Shift Activity** screen, populated with all the agents you selected in the previous step.

- An alternative way to access the **Add Shift Activity** screen is as follows: choose any agent's shift, then select **Add**, followed by **Activity**. This will open the **Add Shift Activity** pop-up screen, displaying the shift of the agent you initially chose. To include additional agents in the activity, choose **Edit staff**.
Add shift activities in draft or published schedules
3. Select a shift activity from the drop-down.

4. Select an activity type of **Shared** or **Individual**:
   
   a. **Shared** activity: A singular occurrence of the activity is shared among all participating agents. Any modifications made to the activity, such as adjustments to the date or time, will apply to all agents simultaneously.
   
   b. **Individual** activity: Separate instances of the activity will be created for each individual agent. Any modifications made to the activity, such as adjustments to the date or time, will apply to an individual agent.

5. Select the date and time for the activity.

6. Select **Override rules check** if you want the system to ignore rules such as the minimum and maximum working hours exceeded. If unselected, any agent who violates rules due to the addition of this activity will be excluded from the activity. You can review the list of agents that didn't meet the criteria and the specific reasons for their exclusion in the **Actions log**.

7. Select **Optimize shifts for breaks or meals** if you want the system to move any overlapping breaks or meals to a different time. If unselected, any overlapping break or meal will be shortened to accommodate the new activity that is being added.
8. Enter any note in the provided Comment text box.

9. Choose Apply to add the activity to agent schedules.

10. Adding activities to agent schedules using the Optimize shifts for breaks or meals option may take a few minutes to process. You can monitor the progress in the Actions log, where the status will transition from In progress to Complete.

Note

The Actions log is designed to track the status of long running actions, such as adding a shift activity with optimization. The Actions log does not track all changes made to schedules.

Edit a shift activity

1. From an agent's shift, choose the activity, select Edit, and then select the activity name to open the edit activity screen.

2. If the activity was added as a Shared activity, then all of the agents added to the activity will be listed under Staff.
   a. From here, you can add or remove agents, change the date or time of the activity, apply the Override rules check, apply Optimize shifts for breaks or meals again as needed, and add or update Comments.
   b. Choose Apply to commit the changes.

3. If the activity was added as an Individual activity, then only the agent whose shift you chose will be listed under Staff.
   a. From here, you can: change the date or time of the activity, apply the Override rules check, apply Optimize shifts for breaks or meals again as needed, and add or update Comments.
   b. Choose Apply to commit the changes.
Remove a shift activity

1. From an agent’s shift, choose the activity, select **Remove**, and then select the activity name to open the remove activity screen.

2. Choose **Override rules check** or **Optimize shifts for breaks or meals** options as needed.

3. Choose **Remove** to remove the activity.
Time off management

Amazon Connect time off management capabilities enable customers to manage agent time off requests that comply with pre-configured regional labor and business rules. Administrators or managers with the correct security profile permissions will be able to configure the various time off settings. The system will automatically approve or reject requests depending on the configured time off rules and the daily maximum allowed time off hours.

Supervisors or managers with permissions will have the ability to view agent time off requests and can override automatically approved or rejected time off.

Contents

- Enable time off
- Set group allowance for time off
- Create a time off request
- Import an agent's time off balance in a .csv file
- Manager and Agent view request drawer
Enable time off

Enable Time off by selecting the Enable Time off request for this staffing group box for specific Staffing Groups. This is a card in the Staffing Group UI called Request management. After this is selected, the supervisor will see the Make request button in the Published schedule calendar UI.

The following image shows the Request management section of the Staffing Group page.

- **Enable Time off requests for this staffing group**: This option enables the time off management feature for this group of agents and supervisors. Time offs are automatically approved or rejected based on availability of time off allowance.

- **Supervisor approval needed**: If enabled, this lets supervisors manually approve or decline agent time off requests.

![Request management](image)

The following image shows the Published schedule calendar and the location of the Make request option.
Set group allowance for time off

Managers can set the maximum time off hours that agents combined can take within the Forecast Group: by hour, for each calendar day, for specific time off activities.

You use a .csv file to quickly specify time off allowances at a hourly level, for up to 13 months. For example, you might specify Vacation, Personal time off, Casual, and other time off types that you specified when you created shift activities.

Contents

- Download the time off .csv template
- Download time off for a forecast group
- Import group allowance .csv file
- Example of using the time off allowances feature
Download the time off .csv template

1. On the **Scheduling** page, choose the **Time off** tab.
2. On the **Download** dropdown menu, choose **Download template**.

The following image shows an example .csv template that contains valid data.

3. When you add your time off data to the template, note the following:
   
   - Do not change the top row of the .csv file template.
   - In the **Time off activities** column, separate multiple activities with two pipes `||`.
   - The **Start time** and **End time** must have a one-hour duration and set as multiples of 15 minutes. If they do not meet these criteria, the validation will fail when you attempt to upload your .csv file. The example below shows the error message that you might encounter:
     
     Column START_TIME value [2023-08-15T05:01:00] is not a multiple of 15 minutes from top of the hour, such as HH:00, HH:15, HH:30 and HH:45

Download time off for a forecast group

1. On the **Scheduling** page, choose the **Time off** tab.
2. Choose one or more forecast groups that you want in the download csv file.
3. On the **Download** dropdown menu, choose **Current group allowance balance**, as shown in the following image.
The .csv file includes the data that was last uploaded to Amazon Connect. For example, the following image shows the download time off allowance .csv file.

- **LAST_UPLOADED_GROUP_ALLOWANCE_IN_HOURS**: The last upload for Group 1 was 4.4 hours of vacation.
- **GROUP_ALLOWANCE_IN_HOURS** shows they have 2.4 hours remaining in their allowance, they’ve already used 2 hours.

### Import group allowance .csv file

When you upload a .csv file that contains the time off allowance for a forecast group, it overwrites data already in Amazon Connect. For example, if you have 100 agents, and a supervisor uploads data for 20 agents, the data for those 20 agents is overwritten.

For the maximum file size that you can upload, see *File size per upload of time off group allowance data* in *Forecasting, capacity planning, and scheduling feature specifications*.

1. On the **Scheduling** page, choose the **Time off** tab.
2. Choose the Forecast group the group allowance applies to, and then choose **Upload group allowance**. Amazon Connect does the following:
   - Validates the data and provides details if there are errors.
   - Prompts you for confirmation that you want to upload the data.
• Uploads the file and displays a confirmation message when complete.

**Example of using the time off allowances feature**

For example, your business provides time off in December. Here's how you might use the time off allowances feature:

• Managers can allow a group of agents to take *casual leave* and *regular P.T.O* that add up to a maximum of 12 hours on December 20th, from 9AM to 9PM.

• They can automatically decline those types of time off requests on December 22nd by giving a value of 0 - Zero hours.

• Adding value 0 allows them to specify blocked days. Amazon Connect ignores a group allowance check if no value is specified.

This allows the workforce managers to balance an agent's personal time off needs with business headcount needs.

**Create a time off request**

**Supervisor or manager initiated time off request**

1. Supervisors or managers can go to the *Published schedule calendar* view, choose the floating icon on the bottom left and create a time off request. The request drawer opens on the right.
2. Select **Staff** and the time off **Type**. To select a time off range, you can either select **All day** or select specific start and end date times. Select **Override time off rules** if you wish to override the system and allow time off while dismissing group allowance and other rules specified in Staff, Staffing Group or Shift profile rules. Enter a **Reason** and choose **Request**.

3. The request will enter a *pending* state to allow the system to analyze existing rules (even thought rules checks are overridden) and will display a list of any rule failures.

4. The agent will see the pending request in their schedule UI and will receive an in-app notification next to the **Request** icon which displays as an inbox icon at the top right above the metrics view. This allows the agent to view the request details under the **Time off** tab.

5. After the rules validation completes, the time off request status of **Approved** or **Rejected** will be displayed in both the agent and supervisor views.

1 **Tip**

When Amazon Connect evaluates time off requests, it factors in the **Forecast group allowance for time off** and the **individual agent's allowance for time off**, if they've been specified.

**Agent initiated time off request**

Agents can go to the schedule calendar view and choose the floating icon to create a time off request. The request drawer will open and allow the agent to enter details related to their time off request.
Import an agent's time off balance in a .csv file

You can import or export a .csv file of an agent's time off balance. For example, you may download the time off balance from your HR system and then upload it to Amazon Connect.

Amazon Connect uses the time off balance to automatically approve or decline time off requests based on the agent's available net balance.

For the maximum file size that you can upload, see File size per upload of agent time off data in Forecasting, capacity planning, and scheduling feature specifications.

1. Log in to the Amazon Connect admin website with an account that has security profile permissions for Scheduling, Schedule manager - Edit.

   For more information, see Assign permissions.

2. On the Amazon Connect navigation menu, select Analytics and optimization, Scheduling.

3. On the Scheduling page, choose the Staff Rules tab.

4. Choose Download template and store the .csv file on your desktop. It looks similar to the following image.
5. Add data or make changes to the .csv file as needed and then save to your desktop with a new file name.

6. Choose **Upload data** to upload the .csv file. Amazon Connect does the following:
   - Validates the data and provides details if there are errors.
   - Prompts you for confirmation that you want to upload the data.
   - Uploads the file and displays a confirmation message when complete.

After the .csv file is successfully uploaded, Amazon Connect checks the available time off balance when time off requests are submitted. If there is enough time off balance it approves the request. Otherwise, the request is declined.

- The time off balance for the requested time off type must be equal to or greater than the duration of the requested time off.

**Download snapshot**

Choose **Download snapshot** to download the full set of the last uploaded time off balance and the net time off balance as of the time of download.

**How the system calculates time off deductions**

When a staff's time off is approved, the following logic is used to calculate how many hours are deducted from both the staff's time off balance and the group allowance balance:

- If the approved time off period overlaps with one or more staff shifts, then:
  - The system derives the deductible time off hours by taking the total number of overlapped hours and subtracting the duration of shift activities which have the setting **Deduct from time off balance** as Yes.

- If the approved time off period does not have staff shifts that overlap because the schedule for that time period has not been published yet, then:
• The system would check if the staff is scheduled to work on that day based on the shift profile Day (check-box) setting.

• If the staff is not scheduled to work on this day, or if the approved time off is outside of the configured shift profile time window, then no time off hours will be deducted.

• If the staff is scheduled to work on that specific day, the system determines the effective shift length based on the configured shift profile. If the shift length is not explicitly set in the profile, the system defaults to the minimum value between the maximum working hours defined in the Staff Rules for that staff and the shift window duration specified in the shift profile, effectively setting the effective shift length. In the event that there is no Maximum working hours defined for the staff, the system resorts to the shift window duration assigned within the staff's specific shift profile.

• Based on this effective shift duration, the system would then determine which shift activity group would be used to schedule shifts, and then subtract the duration of all shift activities in this group which have the setting Deduct from time off balance as Yes.

Time off deduction logic examples

Workforce managers and supervisors can specify which shift activities, in addition to default work activities, will be counted towards their agents' time-off balance. The following highlights an example of this feature:

There are two time offs configured:

• Vacation time - activity name: VACAY_SK
• Sick time - activity name: SICK_SK

Agent 1 has a vacation (VACAY_SK) balance of 30 hours.

Agent 2 has a sick (SICK_SK) balance of 12 hours.

Agent 3 has a vacation (VACAY_SK) balance of 15 hours.

Agent 1, 2 and 3 have a 6 hours shift. In these shifts, there is a 30 minute Break activity for which Deduct from time off balance is set to NO.
• Agent 1 requested an all day time off (VACAY_SK). Once time off is approved, the system will deduct 5 hours 30 minutes from the current time off balance of 30 hours. 30 minutes for the Break activity will not be deducted because the shift activity flag Deduct from time off balance is set to No. The net balance after time off deduction will become 44 hours and 30 minutes.

• Agent 2 requested time off outside of their shift hours (between 9:15 am – 10:15 am). In this case, given the request is outside of the planned schedule, the system will not deduct from the agent's time off balance.

• Agent 3 requested time off between 2 am to 4am, partially outside of their shift and partially overlapping the shift. The Deduct from time off balance Break activity falls within the time off request. In this scenario, system will deduct 1 hour 15 minutes for the duration between 2:45 am to 4:00 am. The vacation balance for agent 3 would now be 13 hours and 45 minutes.

Manager and Agent view request drawer

At any time supervisors can go to the request drawer under the time off tab and search for an agent by first name, last name or login ID to view all time off requests for a specific agent.
Update / Cancel

A supervisor can cancel or edit a time off request by choosing the **Cancel Request** or **Edit Request** buttons at the bottom of the request drawer window. The following image shows the time off requests from Nikki Wolfe.

An agent will see the updated time off status in their calendar and request drawer. The following image shows the status of Nikki Wolfe's time off requests. Her requests for Sick day off were Accepted.
Overtime management

Simultaneously achieving Service Level (SL), Average Speed of Answer (ASA), and cost targets requires matching supply (# of agents) and demand (# of contacts * handle time). Overtime (OT) and Voluntary Time Off (VTO) are two mechanisms that the contact center management team can deploy to achieve both targets. OT allows handling a contact surge or agent shortages without the need to hire more employees while VTO allows handling a low volume contact period without the expenses of employees in an idle state.

Contents

- Create overtime slots
- Agent accept or decline
- Supervisor override

Create overtime slots

1. Choose the Make Request button in the Published schedule calendar UI and select OT.
2. A supervisor or manager enters the date and time range for overtime.
3. Select the productive activity from the Activity list.

4. Select by Staffing group or by Staff rules.
   - Staffing Groups send a notification to all agents regarding availability of overtime slots. Agents are approved based on a first come, first served model.
   - Staff rules allow supervisors to select specific agents to send overtime notifications to.

5. Select the number of required overtime slots.

6. Provide the reason for requesting overtime in the **Reason** text box. Agents will be able to view the reason prior to accepting or declining the overtime request.

7. Choose **Request**

**Agent accept or decline**

The following image shows pending Overtime requests in the agent calendars. Managers and agents can see overtime requests.

![Overtime requests in agent calendars](image)

Agents can accept or decline overtime in the Agent application schedule calendar.
Required security profile permissions

To accept or decline the request, an agent must have **Agent application schedule calendar - Edit** permissions in their security profile. This permission is shown in the following image of Agent Applications permissions on the security profiles page.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wisdom</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent application schedule calendar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Accept and Decline overtime buttons for agents

The following image shows the Accept and Decline buttons on the agent application.

Supervisor override

Managers can override the system approval for OT/VTO and force Decline a request by clicking on the vertical ellipses next to the agent name. This option is shown in the following image of the **Overtime** pane.
Voluntary time off management

Simultaneously achieving Service Level (SL), Average Speed of Answer (ASA), and cost targets requires matching supply (# of agents) and demand (# of contacts * handle time). Overtime (OT) and Voluntary Time Off (VTO) are two mechanisms that the contact center management team can deploy to achieve both targets. OT allows handling a contact surge or agent shortages without the need to hire more employees while VTO allows handling a low volume contact period without the expenses of employees in an idle state.

Contents

- Create Voluntary time off slots
- Agent accept or decline
- Supervisor override

Create Voluntary time off slots

1. Choose the Make Request button in the Published schedule calendar UI and select VTO.
2. A supervisor or manager enters the date and time range for voluntary time off.
3. Select the productive activity from the Activity list.
4. Select by Staffing group or by Staff rules.
- Staffing Groups send notifications to all agents regarding the availability of overtime slots. Agents are approved based on a first come, first served model.
- Staff rules allow supervisors to select specific agents to send overtime notifications to.

5. Select the number of required voluntary time off slots.

6. Provide the reason for requesting voluntary time off in the **Reason** text box. Agents will be able to view the reason prior to accepting or declining the overtime request.

7. Choose **Request**

**Agent accept or decline**

The contact center manager and agents will see the pending voluntary time off requests in the agent calendars.

Agents can accept or decline voluntary time off (VTO) in the Agent application schedule calendar. In order to accept or decline the request, the agent will need to have **Edit** Security Profile permissions. For more information on Security Profile permissions, see [Update security profiles](#).
Required security profile permissions

To accept or decline the request, an agent must have **Agent application schedule calendar - Edit** permissions in their security profile. This permission is shown in the following image of Agent Applications permissions on the security profiles page.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wisdom</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Agent application schedule calendar</td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Accept and Decline buttons for agents

The following image shows the Accept and Decline buttons on the agent application.

Supervisor override

Managers can override the system approval for OT/VTO and force Decline a request by clicking on the vertical ellipses next to the agent name. This option is shown in the following image of the **Overtime** pane.
Schedule Adherence

Contact center supervisors or managers track schedule adherence to understand when agents are following the schedule that you have created. This helps ensure you achieve your service level targets, while improving agent productivity and customer satisfaction.

Amazon Connect begins generating schedule adherence automatically as soon as a published schedule starts that has shift activities where Adherence = yes.

You can view Schedule Adherence metrics on the **Historical metrics** and **Real-Time metrics** pages. The Schedule Adherence metrics are:

- Adherent time
- Adherence
- Schedule time
- Non-adherent time.

The following image shows an example of choosing Schedule Adherence metrics to appear in a historical metrics report.
Getting started:

1. Schedule Adherence requires that schedules are created and published. For more information, see [Scheduling in Amazon Connect](#).

2. Ensure you have the right permissions to access metrics and scheduling information. For more information on the required permissions, see [security profile permissions for forecasting, capacity planning, and scheduling](#).

Historical Schedule Adherence

This section describes the values used when calculating Historical Schedule Adherence.

Adherence

Percentage of time that an agent correctly follows their schedule. This is measured by tracking if an agent is in an *Available* agent status when they should be in productive state. This percentage is calculated as follows:

\[
\text{Adherence} \% = \left( \frac{\text{Total Adherent Minutes}}{\text{Total Scheduled Adherence Minutes}} \right)
\]

An agent is considered adherent if the agent is in an *Available* Status, when the shift activity is Productive, or if the agent is in Non-Productive Status (i.e Custom Status), when the shift activity is Non-Productive. Otherwise the agent is considered non-adherent. This means that if a shift...
activity is called *Lunch* but marked as productive, the agent is considered adherent if they are in the *Available* agent status.

- Type: String
- Min value: 0.00%
- Max value: 100.00%
- Category: Agent activity-driven metric

**Note**

Anytime you change the schedule, Schedule Adherence is re-calculated up to 30 days in the past from the current date (not the date of the schedule), if schedules are changed.

### Adherent time

Total time an agent was in an *Available* status when their shift activity is productive or was in non-productive status when the shift activity is non-productive.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric

### Non-Adherent time

Total time an agent was not in an *Available* status when their shift activity is productive or not in a non-productive status when their shift activity is non-productive.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric

### Scheduled time

Total time an agent was scheduled (either for productive or non-productive time) and Adherence for those shifts were set to Yes.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric
Real-Time Schedule Adherence

Real-Time agent adherence is available in a table called Agent schedule adherence. You can select this table from both the real-time metrics landing page or within an existing report. This table has the same functionality as an existing agent's table with the following additions.

**Note**
The real-time adherence data may take up to 3 minutes to refresh, but it will capture the complete duration of adherence or non-adherence.

**Real-Time agent adherence status**
- This will indicate whether an agent is adherent or non-adherent in near real-time. For a definition of schedule adherence, see Schedule Adherence.

**Scheduled status**
- This will indicate whether an agent is scheduled to be in productive time or non-productive time. If an agent is not scheduled, it will show as blank.

**Agent adherence duration**
- The amount of time an agent has currently been adherent or non-adherent. When an agent changes between non-adherent or adherent, this value will reset, as it represents the current amount of time.

**Agent adherence percentage**
- The percentage of time an agent has been adherent to their schedule. For a definition of agent adherence percentage, see Historical Schedule Adherence.

**Schedule adherence usage examples**

**Shift activities that are tracked for adherence**
Any shift activity that is marked as Adherence = Yes. If a shift is marked as Adherence = No, adherence is not calculated for that shift.

**How to determine which Agent State an agent should be in for each activity**

If an activity is marked as productive, an agent needs to be in an *Available* agent state. Productivity is determined by the agent being in an available state and is not impacted if the agent isn’t handling live contacts. For tracking how many contacts an agent has handled, see the occupancy metric.

If an activity is marked as non-productive, an agent needs to be in a non-productive custom state. An agent does not have to be in a specific custom state to be considered adherent. For example, if the shift activity is *Lunch*, but the agent switches their status to *Break*, the agent would still be considered adherent since both states are Non-Productive.

**What happens when...**

- **an agent starts working before their schedule starts**

  If an agent does not have a schedule, we do not track adherence for that time. This means that if an agent starts working 5 minutes before or 5 minutes after their schedule, it will not count against their adherence. However, if they decide to leave work 5 minutes early because they started 5 minutes early, they would be considered non-adherent for that 5 minute interval.

- **an agent flips to offline when they are supposed to be a non-productive state**

  This would be considered non-adherent because the agent state is offline, rather than Non-Productive Time.

- **an agent leaves training to answer contacts because of high contact volume**

  In this scenario, the agent would be marked as non-adherent. However, if leaving training is intended, you can adjust the schedule retroactively and adherence will be re-calculated with the new shift.

- **a historical schedule is changed**

  If an agent’s schedule is changed within the last 30 days from the current date (not the date of the schedule), adherence will be re-calculated with the new schedule. This allows making real-time adjustments to an agent's shift and will correctly evaluate their adherence.
Calculating Agent Adherent and Non-Adherent Time

Example

Example 1:
Agent A is scheduled to work from 8:00 to 11:00.

They begin working at 7:30 and then take a break from 10:30 to 11:00. From 7:30 to 8:00 the agent is neither adherent or non-adherent since there is no schedule.

From 8:00 to 10:30 the agent is adherent and from 10:30 to 11:00 the agent is non-adherent because they were in Non-Productive Time when they should have been productive.

This means that Agent A's Adherence was 83%. (Total Adherent Time was 150 minutes/Total Scheduled Time 180 minutes)

Example 2:
Agent B is scheduled to work from 9:00 to 10:30.

They go on Break from 10:30 to 11:00, and then a team meeting from 11:00 to 12:00. They begin working at 9:00 and end up working until 10:45. Then picking the Break custom Non-Productive Time status from 10:45. They forget to switch their status to Team Meeting and leave it as Break until 12:00.

From 9:00 to 10:30 the agent was adherent but from 10:30 to 10:45 the agent was non-adherent because they were in a productive state when they should have been in a non-productive state. From 10:45 to 12:00 they were adherent because they were in a non-productive state the entire time.

This means that Agent B's adherence was 92% (Total Adherent Time: 165 Minutes / Total Scheduled Time: 180 Minutes)

Private optimization APIs

Amazon Connect forecasting, capacity planning, and scheduling uses the following private API resources as actions in its IAM policy:

- connect:BatchAssociateAnalyticsDataSet. Grants access permissions and associates the specified datasets for the specified Amazon Connect instance with the specified AWS account.
• `connect:BatchDisassociateAnalyticsDataSet`. Revokes access permissions and disassociates the specified datasets for the specified Amazon Connect instance with the specified AWS account.

If you remove these actions from the preview role policy, the forecasting, capacity planning, and scheduling features won't work.
Use real-time caller authentication with Voice ID

Amazon Connect Voice ID provides real-time caller authentication and fraud risk detection which make voice interactions in contact centers more secure and efficient. Voice ID uses machine learning to verify the identity of genuine customers by analyzing a caller's unique voice characteristics. This allows contact centers to use an additional security layer that doesn't rely on the caller answering multiple security questions, and makes it easy to enroll and verify customers without changing the natural flow of their conversation. Voice ID also offers real-time detection of fraudsters who frequently target your contact center, thereby reducing losses due to fraud.

With Amazon Connect Voice ID you can:

- Passively enroll customers for voice authentication without requiring them to repeat a particular word or phrase.
- Migrate customers into Voice ID by enrolling them in batch.
- Verify the enrolled customer's identity by analyzing their unique voice characteristics.
- Detect fraudsters from a watchlist that you have created.
- Detect voice spoofing.

How Voice ID works

Customer enrollment

1. When a customer calls for the first time, the agent confirms the identity of the caller by using existing security measures, such as asking for mother's maiden name or a one-time passcode (OTP) delivered by SMS. This ensures that only genuine customers are enrolled in Voice ID.

2. Voice ID starts listening to the customer's speech after the contact has encountered the Set Voice ID block, where Voice ID is enabled. Voice ID listens to the call until one of the following happens:
   - It gets enough audio to evaluate the speaker for authentication, fraud, and enroll the speaker (if requested). This is 30 seconds of customer speech, excluding silence.
   - The call ends.

3. Voice ID then creates the enrollment voiceprint. A voiceprint is a mathematical representation that implicitly captures unique aspects of an individual's voice such as speech rhythm, pitch, intonation, and loudness.
The caller does not need to say or repeat any specific phrases to enroll in Voice ID.

Customer authentication

1. When the enrolled customer calls back in, they are verified through an interaction with an IVR, or during their interaction with an agent.

   By default Voice ID is configured to require 10 seconds of a caller's speech to authenticate, which can be done as part of a typical customer interaction in the IVR or with the agent (such as "what's your first and last name?" and "what are you calling about?"). You can adjust the amount of required speech using the **Authentication response time** property in the Set Voice ID block.

2. Voice ID uses the audio to generate the caller's voiceprint and compares it with the enrolled voiceprint corresponding to the claimed identity, and returns an authentication result.

For more information about the agent's experience, see Use Voice ID.

How much speech is needed for enrollment and authentication

- **Enrollment**: 30 seconds of customer net speech (speech that excludes any silence) to create a voiceprint and enroll a customer.

- **Verification**: By default, 10 seconds of customer net speech to verify that the voice belongs to the claimed identity. The speech can be from interacting with an IVR or an agent. You can adjust the amount of required speech using the **Authentication response time** property in the Set Voice ID.

Batch enrollment

You can get a jump start on using biometrics by batch enrolling customers who have already consented for biometrics. Using stored audio recordings in your S3 bucket, and a JSON input file that provides the speaker identifier and a link to the audio recordings, you can invoke the Voice ID batch APIs.

For more information, see Batch enrollment using audio data from prior calls.
Known fraudster detection

There are a few steps to setting up the real-time detection of fraudsters:

1. Create a new watchlist for storing known fraudsters. Or, use the default watchlist that is created when Voice ID is enabled.
2. Register fraudsters to the new watchlist or the default watchlist.
3. In the Set Voice ID block, specify which watchlist you want to use.

When one of the fraudsters from the watchlist that is specified in the flow calls your contact center, Voice ID analyzes the call audio to return a risk score and outcome. This score indicates how closely the caller's voiceprint matches that of the fraudster's in the watchlist. Voice ID requires 10 seconds of audio to evaluate the call audio for fraud risk from known fraudsters.

Default watchlist

When the Voice ID domain is created, Voice ID creates a default fraudster watchlist for that domain. The name and description of the default fraudster watchlist is encrypted using the KMS key that is provided in the domain and saved in Voice ID.

If you don't provide the fraudster watchlistId for fraud detection or fraudster registration, Voice ID uses the default fraudster watchlist.

You cannot update the metadata of the default fraudster watchlist, but you can associate or disassociate fraudsters from it.

Note

If your Voice ID domain was created before March 2023, when fraudster watchlists was launched: a default watchlist was created and all existing fraudsters have been placed in it.

Voice spoofing detection

1. When a prospective fraudster tries to spoof caller audio using audio playback or synthesized speech, Voice ID returns a risk score and outcome to indicate the how likely it is that the voice is spoofed.
2. By enabling fraud detection in flows, you also enable checks for known fraudster risks and voice spoofing risks.

3. Voice ID requires 10 seconds of audio to evaluate the call audio for fraud risk from voice spoofing.

What data is stored?

Voice ID stores audio files of the speaker's voice, voiceprints, and speaker identifiers. This data is encrypted using a KMS key that you provide.

If you enable detection of fraudsters in a watchlist, Voice ID also stores the fraudster audio and voiceprints. For more information, see Data handled by Amazon Connect.

Voice ID domains

When you enable Amazon Connect Voice ID, you create a Voice ID domain: a container for all Voice ID data, such as speaker identifiers (which serves as the customer identifier), the voiceprints, the customer audio that was used for creating the enrollment voiceprints, and the enrollment statuses (enrolled, opted out, etc.) associated with the speaker identifiers. For detection of fraudsters in a watchlist, the Voice ID domain stores the fraudster identifiers, voiceprints, and audio used for creating the voiceprints.

Following are guidelines for creating Voice ID domains:

- Each Amazon Connect instance can be associated with only one Voice ID domain.
- Each Voice ID domain can be associated with multiple Amazon Connect instances. This enables you to use the same stored customer data across multiple Amazon Connect instances.
- You can create multiple domains, but they don't share customer data between each other.
- We recommend creating a new Voice ID domain to associate with a Amazon Connect instance when:
  - You are enabling Voice ID for the first time on your account in an AWS Region.
  - You want to ensure that you isolate the Voice ID domains used for your test and production environments.
- We recommend using an existing Voice ID domain when:
  - You want to use the same set of enrolled callers and fraudsters across different Amazon Connect instances (that may belong to different customer service teams)
• You want to use the same test environment across different test Amazon Connect instances.

Note

Only existing Voice ID domains in the same Region in your Amazon Connect account can be shared across Amazon Connect instances in that Region.

• You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain.

• To delete a Voice ID domain, use the **DeleteDomain** Voice ID API. DeleteDomain soft deletes the domain. Amazon Connect waits 30 days before completely erasing the domain data. During this period, Voice ID is disabled for all the Amazon Connect instances it is associated with. To restore a domain during this window, submit an AWS Support ticket and provide the domain ID. You can find the domain ID on the Voice ID section of the Amazon Connect console, as shown in the following example:

Deleting a Voice ID domain deletes all stored customer data, such as audio recordings, voiceprints, and speaker identifiers, as well as any fraudster watchlists that you managed.

**Enrollment status**

Voice ID stores three different enrollment status for a speaker: ENROLLED, OPTED_OUT and EXPIRED. You can recall these speaker status using Amazon Connect Voice ID APIs and using contact flow blocks to take appropriate action.
• **ENROLLED**: When you enroll a new caller is enrolled into Voice ID, Voice ID creates a new voiceprint and set the speaker status as ENROLLED. Even if you re-enroll the same caller into Voice ID, the status stays as ENROLLED.

• **OPTED_OUT**: If a caller does not provide consent to enroll into biometrics, you can opt out the caller (in the Contact Control Panel) or using APIs. Voice ID creates a new entry for this caller and set the speaker's status OPTED_OUT. Voice ID does not generate any voiceprint or store any audio recording for the speaker. Future enrollment requests for this speaker is rejected unless their entry is deleted.

• **EXPIRED**: If a caller's voiceprint has not been accessed or refreshed for 3 years, Voice ID changes the status to EXPIRED, and you are no longer able to perform authentications for this caller. You can re-enroll the caller again or delete the caller from Voice ID.

## Expired speakers

For BIPA compliance, Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years.

To view a speaker’s last access, look at the `lastAccessedAt` attribute that is returned by the `DescribeSpeaker` and `ListSpeakers` APIs.

If you try to use the `EvaluateSession` API to authenticate an expired speaker, a `SPEAKER_EXPIRED` authentication decision is returned.

To use the expired speaker again, they must be re-enrolled.

## Speaker and fraudster identifiers

Voice ID uses speaker identifiers to refer to and retrieve the voiceprints in a Voice ID domain. We recommend that you use identifiers that do not contain an Personally Identifiable Information (PII) in the identifiers.

Voice ID creates two fields to refer to a caller:

- **CustomerSpeakerId**: A identifier provided by the customer. It can be between 1-256 characters and can only contain: `a-z, A-Z, 0-9, - and _`

- **GeneratedSpeakerId**: A unique 22-character alphanumeric string that Voice ID creates and returns at the time of enrollment of the caller.
Amazon Connect Voice ID speaker APIs accept either form of speaker identifiers, but only emit GeneratedSpeakerId in the Voice ID event streams and contact records. If you want to re-record the caller to redo the voiceprint, you can enroll the caller with the same CustomerSpeakerId.

Similarly, Voice ID creates unique fraudster identifiers called GeneratedFraudsterID for every fraudster that you add to a watchlist in the domain. Voice ID returns the fraudster identifier if a fraudster is detected in a call when performing fraud risk detection.

Enable Voice ID

Before you begin

Before you get started, complete the following tasks.

Tasks

- Grant the required permissions
- Decide how to name your Voice ID domain
- Create an AWS KMS key to encrypt data stored in the domain

Grant the required permissions

You must grant the required permissions to users, groups, or roles. For more information, see AmazonConnectVoiceIDFullAccess.

Access to Voice ID APIs using the Contact Control Panel (CCP) is disabled by default.

Decide how to name your Voice ID domain

When you enable Voice ID, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, Voice ID-ExampleCorp.

Create an AWS KMS key to encrypt data stored in the domain

When you enable Voice ID, you are prompted to create or provide an AWS KMS key. It encrypts the customer data stored by Voice ID such as audio files, voiceprints, and the speaker identifiers.

Step-by-step instructions for creating these KMS keys are provided in Step 2: Create a new Voice ID domain and encryption key.
Data at rest—specifically, freeform fields that you provide plus audio files/voiceprints—are encrypted under the KMS key you choose. Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

When making calls to Voice ID for anything other than CreateDomain or UpdateDomain, the user making the call requires kms:Decrypt permissions for the key associated with the domain. When making calls to CreateDomain or UpdateDomain, the user also requires kms:DescribeKey and kms:CreateGrant permissions for the key. When you create (or update) a Voice ID domain, it creates a grant on the KMS key so that it can be used by Voice ID asynchronous processes (such as speaker enrollment) and by the Amazon Connect service-linked role during your flows. This grant includes an encryption context specifying the domain with which the key is associated. For more on grants, see Using grants in the AWS Key Management Service Developer Guide.

If you create a domain and associate it with one key, store some data, and then change the KMS key to a different key, an asynchronous process will be triggered to re-encrypt the old data with the new KMS key. After this process completes, all of your domain's data will be encrypted under the new KMS key, and you may safely retire the old key. For more information, see UpdateDomain.

Tip
You can create KMS keys or provide an existing KMS key programmatically. For more information, see Amazon Connect Voice ID APIs.

Step 1: Read the BIPA Consent Acknowledgement

Reading the Biometric Privacy Act (BIPA) Consent Acknowledgement is a requirement to enable Voice ID. You need to do this once per account, across all Regions. You cannot do this step by using APIs. For more information about BIPA, see this Wikipedia article: Biometric Information Privacy Act.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.
3. In the navigation pane, choose **Voice ID**. Read the BIPA Consent Acknowledgement, and accept if you agree.

### Step 2: Create a new Voice ID domain and encryption key

You can perform this step using the Amazon Connect console or by using Amazon Connect and Voice ID APIs.

**Amazon Connect console instructions**

1. In the **Domain setup** section, choose **Create a new domain**.
2. In the **Domain name** box, enter a friendly name that's meaningful to you, such as your organization name, for example, *VoiceID-ExampleCorp*.

3. Under **Encryption**, create or enter your own AWS KMS key for encrypting your Voice ID domain. Following are the steps to create your KMS key key:

   1. **Choose Create KMS key.**

   2. A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.
3. On the **Add labels** page, add a name and description for the KMS key, and then choose **Next**.

4. On the **Define key administrative permissions** page, choose **Next**.

5. On the **Define key usage permissions** page, choose **Next**.

6. On the **Review and edit key policy** page, choose **Finish**.

7. Return to the tab in your browser for the Amazon Connect console, **Voice ID** page. Click or tap in the **AWS KMS key** for the key you created to appear in a dropdown list. Choose the key you created.

4. Choose **Enable Voice ID**.

**API instructions**

1. Call the [CreateDomain](#) API to create a new Voice ID domain.

2. Call the [CreateIntegrationAssociation](#) API to associate the Voice ID domain with the Amazon Connect instance.
   - Pass the ARN of the Voice ID domain just created into the `IntegrationArn` parameter. For `IntegrationType` use `VOICE_ID`.

You've enabled Voice ID for your instance. The following has been created:

- Your Voice ID domain and a default fraudster watchlist that will hold your fraudsters.
• A managed Amazon EventBridge rule in your account. This rule is used to ingest Voice ID events for creating contact records related to Voice ID. Additionally, Amazon Connect adds Voice ID permissions to the service-linked role for Amazon Connect.

Next, in Step 3 you configure how you want Voice ID to work in your flow.

**Step 3: Configure Voice ID in your contact flow**

In this step you add the required blocks to your flow and configure how you want Voice ID to work.

- **Play prompt**: Add this block before the Set Voice ID block to stream audio properly. You can edit it to include a simple message such as "Welcome."
- **Set Voice ID**: After the Play prompt block, add the Set Voice ID block. It should be at the start of a call. Use this block to start streaming audio to Amazon Connect Voice ID to verify the caller's identity, as soon as the call is connected to a flow.

  In Set Voice ID block you configure the authentication threshold, response time, fraud threshold, and fraudster watchlist to be used for known fraudster detection.

- **Set contact attributes**: Use to pass the CustomerId attribute to Voice ID. The CustomerId may be a customer number from your CRM, for example. You can create a Lambda function to pull the unique customer ID of the caller from your CRM system. Voice ID uses this attribute as the CustomerSpeakerId for the caller.

  ![Note]
  
  CustomerId can be an alphanumeric value. It supports only _ and - (underscore and hyphen) special characters. It does not need to be UUID. For more information, see CustomerSpeakerId in the Speaker data type.

- **Check Voice ID**: Use to check the response from Voice ID for enrollment status, voice authentication, and fraud detection, and then branch based on one of the returned statuses.

**Example Voice ID flow**

**Caller not enrolled**

1. When a customer calls for the first time, their CustomerId is passed to Voice ID using the **Set contact attributes** block.
2. Voice ID looks for `CustomerId` in its database. Since it's not there, it sends a **Not enrolled** result message. The Check Voice ID block branches based on this result, and you can decide what the next step should be. For example, you might want agents to enroll the customer in voice authentication.

3. Voice ID starts listening to the customer's speech after the contact has encountered the Set Voice ID block, where Voice ID is enabled. It listens until it accumulates 30 seconds of net speech or the call ends, whichever happens first.

**Caller enrolled**

1. The next time the customer calls, Voice ID finds their `CustomerId` in the database.

2. Voice ID starts listening to the audio to create a voiceprint. The voiceprint that is created this time is used for authentication purposes so Voice ID can compare if the caller had been enrolled previously.

3. It compares the caller's current voiceprint with the stored voiceprint associated with the claimed identity. It returns a result based on the **Authentication threshold** property you configured in the Set Voice ID block.

4. After it evaluates the speech, it returns the message **Authenticated** if the voiceprints are similar. Or it returns one of the other statuses.

5. The contact is then routed down the appropriate branch by the Check Voice ID block.

**Security profile permissions for Voice ID**

- To enable users to search for contacts by their Voice ID status, assign the following **Analytics and Optimization** permission to their security profile:
  - **Voice ID – attributes and search**: Enables users to search for and view Voice ID results on the Contact detail page.

- To grant agents access to Voice ID in the Contact Control Panel, assign the following permission in the **Contact Control Panel** group:
  - **Voice ID – Access**: Enables controls in the Contact Control Panel so agents can:
    - View authentication outcomes.
    - Opt-out or re-authenticate a caller.
    - Update SpeakerID.
• View fraud detection results, rerun fraud analysis (fraud detection decision, fraud type and score).

Note

The functionality to enter or update the SpeakerID is not available with the default Voice ID widget in the CCP. To include the option for updating the SpeakerID, implement the updateVoiceIdSpeakerId Amazon Connect Streams API in your custom CCP.

The following image shows an example of these controls on the CCP:

![Voice ID control panel]

For information about how to add more permissions to an existing security profile, see Update security profiles.

By default, the Admin security profile already has permissions to perform all Voice ID activities.

Search and review Voice ID results

Use the Contact search page to search for and review the results of enrollment status, voice authentication, and detection of fraudsters in a watchlist. With the required security profile permissions (Analytics and Optimization - Voice ID - attributes and search - View), you can search for Voice ID results using the following filters:

• **Speaker actions**: Use this filter to search for contacts where the caller was enrolled into Voice ID or chose to opt-out of Voice ID altogether.

• **Authentication result**: Use this filter to search for contacts where Voice ID authentication returned the following results:
• Authenticated
• Not authenticated
• Opted out
• Inconclusive
• Not enrolled

For example, if you want to search for all contacts where the authentication status was returned as **Not authenticated** or **Opted out**, select both these options and choose **Apply**.

• **Fraud detection result**: Use this filter to search for contacts where Voice ID fraud analysis returned the following results:
  • High risk for fraud
  • Low risk for fraud
  • Inconclusive

• **Fraud detection reason**: Use this filter to search for contacts where specific fraud risk mechanisms were detected:
  • Known fraudster: the caller’s voice matches a fraudster from the fraudster watchlist you have created.
  • Voice spoofing: the caller is modifying their voice or is using speech synthesis to spoof the agent.

**Voice ID results in a contact record**

After you search for a contact, you can choose an ID to view their contact record. The following image shows an example of the fields in the Voice ID section of the contact record:
Use the Voice ID APIs

To manage Voice ID programmatically, see Amazon Connect Voice ID APIs.

This section explains how to perform common scenarios using the Voice ID APIs.

Contents

- Voice ID domain operations
- Voice ID and Amazon Connect Integration Association APIs
- Voice ID speaker, watchlist, and fraudster management APIs
- Batch enrollment using audio data from prior calls
- Input and output file schema for Speaker Enrollment Job
- Create and edit a fraudster watchlist
- Input and output file schema for Fraudster Registration Job
- Amazon Connect Streams Voice ID APIs

Voice ID domain operations

Amazon Connect Voice ID provides APIs for you manage Voice ID domains. You can find equivalents for Create, Describe, List, and Update in the AWS Console.
1. **CreateDomain**: To create a new Voice ID domain, use the CreateDomain Voice ID API. When the Voice ID domain is created, a default fraudster watchlist to hold your fraudsters is created at the same time.

   Note the following guidelines when using the CreateDomain API:
   - You can only invoke this for your account after you have acknowledged the BIPA Consent in the AWS console.
   - You must also specify the KMS key for the Voice ID domain at the time of creation.
   - After creating a Voice ID domain, use the [Amazon Connect association APIs](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/voice-id-association-apis.html) to associate it with an Amazon Connect instance.

2. **DeleteDomain**: To delete a Voice ID domain, you must invoke the DeleteDomain Voice ID API and provide the domain ID. If this domain was associated with an Amazon Connect instance, Voice ID API calls, and Voice ID flow blocks will return runtime error. Deleting a Voice ID domain deletes all stored customer data such as audio recordings, voiceprints and speaker identifiers, as well as fraudster lists that you managed.

3. **DescribeDomain**: Use this API to return the name, description and encryption configuration of an existing domain identified by its DomainID.

4. **ListDomains**: Use this API to list all your Voice ID domains owned by your account in the Region.

5. **UpdateDomain**: To update the name and encryption configuration for a domain, you can use the UpdateDomain Voice ID API. This API clobbers existing attributes, and you must provide both these fields.

   When you change the KMS key associated with the Voice ID domain, following the UpdateDomain call your domain's existing data will be asynchronously re-encrypted under the new KMS key. You can check status of this process from your domain's ServerSideEncryptionUpdateDetails attribute using the DescribeDomain API. While this update process is in progress, you must retain your old KMS key in an accessible state, otherwise this process may fail. After this process completes, the old KMS key may be safely retired.

### Voice ID and Amazon Connect Integration Association APIs

You can use the following APIs to manage associations with Amazon Connect instances. You can perform these operations on the AWS Console as well.
1. **CreateIntegrationAssociation**: To enable Voice ID on an Amazon Connect instance, you will need to associate a Voice ID domain with an Amazon Connect instance using a CreateIntegrationAssociation request. You can only associate one Voice ID domain to an Amazon Connect instance. If the instance is already associated with a domain, the API returns the following error:

DuplicateResourceException (409) - Request is trying to create a duplicate resource.

2. **DeleteIntegrationAssociation**: To delete an existing association between an Amazon Connect instance and a Voice ID domain, you will need to call the DeleteIntegrationAssociation APIs along with the Amazon Connect InstanceID and the IntegrationAssociationID returned by CreateIntegrationAssociation. This is a required step if you want to associate a different Voice ID domain to this Amazon Connect instance. We do not recommend deleting associations in a production setup as it can cause unpredictable behavior for Voice ID in your Amazon Connect instance.

3. **ListIntegrationAssociations**: To list all the associations between Amazon Connect instance and Voice ID domains for your account in this Region, you can invoke ListIntegrationAssociations API.

**Voice ID speaker, watchlist, and fraudster management APIs**

Amazon Connect Voice ID includes APIs to manage speakers enrolled into a Voice ID domain and fraudsters registered in the domain. All speaker APIs, except ListSpeakers, accept either the CustomerSpeakerId or GeneratedSpeakerId.

**Speaker management APIs**

1. **DescribeSpeaker**: Describe a speaker's status in a domain (ENROLLED, OPTED_OUT, EXPIRED), and to map a GeneratedSpeakerId to a CustomerSpeakerId, and vice versa.
2. **DeleteSpeaker**: Completely remove all records for a caller/speaker from a Voice ID domain. All voiceprints and enrollment status is deleted immediately, and associated audio recordings are removed within 24 hours.

3. **ListSpeakers**: List all the speakers whose entries are present in a Voice ID domain. This API returns both the CustomerSpeakerId and GeneratedSpeakerId for a speaker. It returns a paginated output with the page size dictated in the API request.

4. **OptOutSpeaker**: Opt out a caller from a Voice ID domain. This API doesn't require the speaker to be present in Voice ID. A non-existing speaker can be opted-out using this API and Voice ID persists the opted out status and rejects future enrollment requests for this speaker. Opting out also removes voiceprints and any stored audio recordings for this caller.

**Watchlist management APIs**

1. **CreateWatchlist**: Create a watchlist that fraudsters can be a part of.

2. **DeleteWatchlist**: Remove a custom fraudster watchlist from the Voice ID domain. To delete a watchlist, it must be empty. That is, it must not have any fraudsters associated to it. You can use the **DeleteFraudster** or **DisassociateFraudster** APIs to remove all fraudsters from a watchlist.

   You cannot delete the default watchlist from a Voice ID domain.

3. **DescribeWatchlist**: Determine if it is a default fraudster watchlist, or a custom watchlist that you created, and obtain watchlist details.

4. **ListWatchlists**: List all the watchlists in the Voice ID domain.

5. **UpdateWatchlist**: Update the name and description of a custom fraudster watchlist. You cannot modify details of the default watchlist because it's managed by Voice ID.

**Fraudster management APIs**

1. **AssociateFraudster**: Associate a fraudster to a watchlist in the same domain. You can associate a fraudster to multiple watchlists in a domain.

2. **DeleteFraudster**: Delete a fraudster from a Voice ID domain. Deleting the fraudster removes the fraudster from all watchlists it is a part of. It also deletes all voiceprints and associated audio recordings within 24 hours.

3. **DescribeFraudster**: Describe a fraudster's status in the Voice ID domain.
4. **DisassociateFraudster**: Disassociate a fraudster from the watchlist specified. Note that a fraudster always has to be associated with at least one fraudster watchlist; an exception is thrown if you try to disassociate a fraudster from its only watchlist.

To remove the fraudster completely, use **DeleteFraudster**.

5. **ListFraudsters**: List all the fraudsters in a domain or a specific watchlist. This API also returns the watchlists the fraudster is a part of. It returns a paginated output with the page size dictated in the API request.

**Batch enrollment using audio data from prior calls**

You can get a jump start on using biometrics by batch enrolling customers who have already consented for biometrics. Using stored audio recordings in your S3 bucket, and a JSON input file that provides the speaker identifier and a link to the audio recordings, you can invoke the **Voice ID batch** APIs.

To enroll customers programmatically, pass the following data to the API:

1. The domain ID to specify the domain to associate recordings to.

2. The location for the output file.

3. An input file containing a list of speakers. See [Input and output file schema for Speaker Enrollment Job](#).

   For each speaker the file must include:

   - A link to a call audio recording in a .wav file with 8KHz sample rate and PCM-16 encoding.
   - The corresponding `CustomerSpeakerId` for the customer.
   - A channel for the caller in the audio recording. If the audio has multiple channels, you can select only one.

4. A KMS key to use when writing the output.

5. A role that **Voice ID** can assume. It must have access to the S3 bucket where the audio files are stored. This role must have access to any KMS key used to encrypt the files. It must also be able to write to the specified output location and use the KMS key requested for writing the output. Specifically, it must have the following permissions:

   - `s3:GetObject` on the input bucket.
   - `s3:PutObject` on the output bucket.
• `kms:Decrypt` on the KMS key used for input bucket's default encryption.
• `kms:Decrypt` and `kms:GenerateDataKey` on the KMS key provided in the input which will be used for writing output file to the output bucket.

You must have `iam:PassRole` permissions when making the call and providing the `dataAccessRole`. To enable confused deputy protection for the `dataAccessRole`, see [Amazon Connect Voice ID cross-service confused deputy prevention](#).

6. Optionally, a fraud check skip flag in case you want to skip checks for fraud and voice spoofing on the enrollment audio.

7. Optionally, specify a fraudster watchlist that you want to perform fraud checks against. If no watchlist is specified, Voice ID uses the default fraudster watchlist for the domain.

8. Optionally, the fraud threshold in case you want to raise or lower the risk.

9. Optionally, a flag to re-enroll enrolled customers. This is useful if you want to refresh the audio recording, since the default is to ignore previously enrolled customers.

The batch enrollment returns the `CustomerSpeakerId`, `GeneratedSpeakerId`, and associated status for each entry. It stores this data in a JSON file at the output path you specify in the API.

⚠️ **Note**
You are charged for enrolling speakers. For more information, see [Amazon Connect Voice ID Pricing](#).

### Input and output file schema for Speaker Enrollment Job

#### Input file schema

Following is the schema of the input manifest file for the Speaker Enrollment Job:

```json
{
   "Version": "string",
   "SpeakerEnrollmentRequests": [
      {
         "RequestId": "string",
         "SpeakerId": "string",
         "AudioSpecifications": [
            {
               ...
            }
         ]
      }
   ]
}
```
Following is a description of each attribute of the input schema.

- **Version**: The version of the input schema document. Currently, this should be `1.0`.
- **SpeakerEnrollmentRequests**: List of speaker enrollment requests to be fulfilled as part of the job.
  - **RequestId**: An identifier for this speaker enrollment request. It must be unique within the input file. It is used for mapping and identifying entries in the output file.
  - **SpeakerId**: The client-provided identifier of the speaker who needs to be enrolled. You must pass the `CustomerSpeakerId` in this field. The `GeneratedSpeakerId` is not currently supported.
  - **AudioSpecifications**: The list of audio files that Voice ID can use for enrolling this speaker. Voice ID uses these audio files together to gather required amount of speech for enrollment. Currently, the maximum number of audio files allowed for an enrollment request is `10`. Each file can be a .wav file up to 20MB, containing audio with 8KHz sample rate and PCM-16 encoding.
  - **S3URI**: The Amazon S3 location of the audio file in .wav format that needs to be used for enrolling the speaker.
  - **ChannelId**: The audio channel to be used for enrolling the speaker in a multi-channel audio file. Voice ID supports audio files with up to two channels, so this value is restricted to either `0` or `1`.

**Output file schema**

Following is the schema of the output file generated for the Speaker Enrollment Job:
Following is a description of each attribute of the output schema.

- **Version**: The version of the output schema document. Currently, this should be 1.0.
- **Errors**: The list of errors for the speaker enrollment requests that failed at some point during enrollment.
- **RequestId**: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.
- **ErrorCode**: The HTTP error code representing the type of error. Some example error scenarios are described below.

  **Note**
  This is not an exhaustive list.

- **400 (Bad Request Exception):**
  - The input JSON file is malformed and cannot be parsed.
  - The provided audio files do not have enough speech for enrollment.
  - Fraud verification checks failed for the given speaker.
- 402 (ServiceQuotaLimitExceededException):
  - Speaker limit exceeded.
- 409 (Conflict Exception):
  - Conflicting action: You cannot request an enrollment for an opted out speaker.
- 500 (Internal Failure):
  - Internal Server Error (Unexpected error on the Service-side).
- ErrorMessage: A message describing the cause of the enrollment failure.
- SuccessfulEnrollments: The list of enrollment requests that succeeded.
  - RequestId: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.
  - CustomerSpeakerId: The client-provided identifier for the speaker who was enrolled.
  - GeneratedSpeakerId: The service-generated identifier for the speaker who was enrolled.
  - EnrollmentStatus: The status of successful speaker enrollment
    - DUPLICATE_SKIPPED: The speaker is already enrolled, and the enrollment was skipped.
    - NEW_ENROLLMENT: The speaker was newly enrolled into the system.
    - ENROLLMENT_OVERWRITE: The speaker is already enrolled, but was re-enrolled/overwritten using the new audio.

Create and edit a fraudster watchlist

Use the following APIs to create a fraudster watchlist and register fraudsters:

1. Use the CreateWatchlist API to create new fraudster watchlists.
2. Use the StartFraudsterRegistrationJob API for batch registration. You can register new fraudsters to the new watchlist, or register them to the default watchlist that is associated with the Voice ID domain.

When registering a new fraudster, Voice ID compares the voiceprint against all registers fraudsters in your Voice ID domain to determine if it is a duplicate of an existing fraudster.

To add fraudsters to a specified fraudster watchlist, pass the following data to the API:

1. The domain ID to specify the domain to associate recordings to.
2. An input file containing a list of fraudsters. See Input and output file schema for Fraudster Registration Job.

3. The location for output file.

4. A KMS key to use when writing the output.

5. A role that Voice ID can assume. It must have access to the S3 bucket where the audio files are stored. This role must have access to any KMS key used to encrypt the files. It must also be able to write to the specified output location and use the KMS key requested for writing the output. Specifically, it must have the following permissions:
   - s3:GetObject on the input bucket.
   - s3:PutObject on the output bucket.
   - kms:Decrypt on the KMS key used for input bucket's default encryption.
   - kms:Decrypt and kms:GenerateDataKey on the KMS key provided in the input which will be used for writing output file to the output bucket.

   You must have iam:PassRole permissions when making the call and providing the dataAccessRole. To enable confused deputy protection for the dataAccessRole, see Amazon Connect Voice ID cross-service confused deputy prevention.

6. A watchlistId to register the fraudster to. If no watchlistId is specified, fraudsters are registered to the default watchlist for that Voice ID domain.

7. The threshold for establishing the duplicate status of fraudsters.

8. A flag to ignore fraudster duplicates.

Voice ID updates the fraudster list with successful additions, and return a GeneratedFraudsterID associated with entry back to the same S3 location. If duplicates are identified, Voice ID returns a "duplicate" status for the entry and provides the closest matching GeneratedFraudsterId. After a fraudster is registered successfully, you can associate this fraudster identified by the GeneratedFraudsterID into a new watchlist by using the AssociateFraudster API.

Voice ID is not able to perform detection of fraudsters in a watchlist before the fraudster list is created.

For quotas for the fraudster list, see Amazon Connect service quotas.
Input and output file schema for Fraudster Registration Job

Input file schema

Following is the schema of the input manifest file for Fraudster Registration Jobs:

```
{
   "Version": "string",
   "FraudsterRegistrationRequests": [
   {
      "RequestId": "string",
      "AudioSpecifications": [
      {
         "S3Uri": "string",
         "ChannelId": number
      }
   ]
   ]
}
```

Note

All the fields in the schema are required.

Following is a description of each attribute of the input schema.

- **Version**: The version of the schema document. Currently, this should be `1.0`.
- **FraudsterRegistrationRequests**: List of fraudster registration requests to be fulfilled as part of the job.
  - **RequestId**: An identifier for this fraudster registration request. It must be unique within the input file. It is used for mapping and identifying entries in the output file.
• **AudioSpecifications**: The list of audio files that Voice ID can use for registering this fraudster. Voice ID uses these audio files together to gather required amount of speech for registration. Currently, the maximum number of audio files allowed for a registration request is **10**. Each file can be a .wav file up to 20MB, containing audio with 8KHz sample rate and PCM-16 encoding.

• **S3URI**: The Amazon S3 location of the audio file in .wav format that needs to be used for registering the fraudster.

• **ChannelId**: The audio channel to be used for registering the fraudster in a multi-channel audio file. Voice ID supports audio files with up to two channels, so this value is restricted to either **0** or **1**.

### Output file schema

Following is the schema of the output manifest file for Fraudster Registration Jobs:

```json
{
    "Version": "string",
    "Errors": [
        {
            "RequestId": "string",
            "ErrorCode": number,
            "ErrorMessage": "string"
        }
    ],
    "SuccessfulRegistrations": [
        {
            "RequestId": "string",
            "GeneratedFraudsterId": "string",
            "RegistrationStatus": "DUPLICATE_SKIPPED" | "NEW_REGISTRATION",
            "FraudsterSimilarityScore": number
        }
    ]
}
```

Following is a description of each attribute of the output schema.

• **Version**: The version of the output schema document. Currently, this should be **1.0**.

• **Errors**: The list of errors for the fraudster registration requests that failed at some point during registration.
• RequestId: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.

• ErrorCode: The HTTP error code representing the type of error. Some example error scenarios are described below.


Note

This is not an exhaustive list.

• 400 (Bad Request Exception):
  • The input JSON file is malformed and cannot be parsed.
  • The provided audio files do not have enough speech for registration.

• 402 (ServiceQuotaLimitExceededCacheException):
  • Fraudster limit exceeded.

• 500 (Internal Failure):
  • Internal Server Error (Unexpected error on the Service-side).

• ErrorMessage: A message describing the cause of the fraudster registration failure.

• SuccessfulRegistrations: The list of registration requests that succeeded.
  • RequestId: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.
  
  • RegistrationStatus: The status of successful fraudster registration.
    • DUPLICATE_SKIPPED: The fraudster was identified as a duplicate, and the registration was skipped.
    • NEW_FRAUDSTER: The Fraudster was newly enrolled into the system.

  • GeneratedFraudsterId: The service-generated identifier for the fraudster who was registered. In case the RegistrationStatus is DUPLICATE_SKIPPED, this is the identifier of the fraudster already in the domain that is the closest match to the given fraudster.

  • FraudsterSimilarityScore: An optional field that is populated when the fraudster registration is skipped due to it being a duplicate. This represents the similarity of the given fraudster with the closest matching fraudster already existing in the domain.
Amazon Connect Streams Voice ID APIs

Use the following Amazon Connect Streams APIs to integrate Voice ID into your existing agent web applications.

- `enrollSpeakerInVoiceId`: Enroll a customer to Voice ID after obtaining their consent to enroll.
- `evaluateSpeakerWithVoiceId`: Check the customer’s Voice ID authentication status, and to detect fraudsters.
- `optOutVoiceIdSpeaker`: Opt out a customer from Voice ID.
- `getVoiceIdSpeakerStatus`: Describe the enrollment status of a customer.
- `getVoiceIdSpeakerId`: Get the SpeakerID for a customer.
- `updateVoiceIdSpeakerId`: Update the SpeakerID for a customer.

You can also use the Voice ID widget in the Contact Control Panel (CCP) if you don't want to build a custom agent interface. For more information about Voice ID in the CCP, see Use Voice ID.

Voice ID event schema

Voice ID generates events for every transaction: enrollment, authentication, or detection of fraudsters in a watchlist. Events are sent to the EventBridge default event bus.

You can create an analytics pipeline for Voice ID authentication outcomes and detection of fraudsters in a watchlist by using EventBridge to monitor Voice ID events. Using the schema available in this topic, you can configure EventBridge rules to listen and filter for Voice ID events that are relevant, and then process them through Amazon Kinesis Data Firehose to store in a data warehouse of your choice.

For example, you may want near real-time tracking of Voice ID analysis. To do that, you can pull all the Evaluate-Session events, and get the authenticationResult and fraudDetectionResult.

Events are emitted on a best effort basis.

Common fields in the event

- `version`: The version of the event data.
• id - A unique identifier of the event generated by EventBridge
• detail-type - An identifier for the details of the event.
• source - The source of the event. This is always aws.voiceid.
• account - AWS account ID.
• timestamp - The date and time that the event was published in UTC.
• region - The AWS Region where the API call was made.
• resources - Resources used by the API call.
• detail - Details about the event:
  • detail.sourceId - A unique ID generated by Voice ID that you can use for de-duplication.
  • detail.action - Analogous to the API being invoked.
  • detail.status - Specifies the status of the action: success or failure.
  • detail.errorInfo - Is populated when the specified action errors out at Voice ID.

Following are the schemas for the events that are emitted.

**Start Session Action**

Emits events on stream start (after setup), stream end, and on failures.

```json
{...commonfields
   "detail-type": "VoiceId Start Session Action",
   "detail": {
       "sourceId": String,
       "action": "START_SESSION",
       "status": String,
       "domainId": String,
       "session": {
           "sessionId": String,
           "sessionName": String,
           "authenticationConfiguration": {
               "acceptanceThreshold": Integer
           },
           "fraudDetectionConfiguration": {
               "riskThreshold": Integer,
               "watchlistId": String
           },
           "streamingConfiguration": {
               "authenticationMinimumSpeechInSeconds": Integer
           }
       }
   }
```

Start Session Action
Update Session Action

Emits events when the internal session update succeeds or fails.

{...commonfields
"detail-type": "VoiceId Update Session Action",
"detail": {
   "sourceId": String,
   "action": "UPDATE_SESSION",
   "status": String,
   "domainId": String,
   "session": {
      "sessionId": String,
      "sessionName": String,
      "authenticationConfiguration": {
         "acceptanceThreshold": Integer
      },
      "fraudDetectionConfiguration": {
         "riskThreshold": Integer,
      }
   }
}}
Evaluate Session Action

Emits events when the session evaluation succeeds or fails. Reasons can be KNOWN_FRAUDSTER or VOICE_SPOOFING.

```json
...
"detail-type": "VoiceId Evaluate Session Action",
"detail": {
    "sourceId": String,
    "action": "EVALUATE_SESSION",
    "status": String,
    "domainId": String,
    "session": {
        "sessionId": String,
        "sessionName": String,
        "generatedSpeakerId": String,
        "streamingStatus": String,
        "authenticationResult": {
            "authenticationResultId": String,
            "decision": String,
            "score": Integer,
            "audioAggregationStartedAt": "Timestamp",
            "audioAggregationEndedAt": "Timestamp",
            "configuration": {
                "acceptanceThreshold": Integer
            }
        },
        "fraudDetectionResult": {
```
Speaker Action

Emits events on the success or failure to opt out a speaker, delete a speaker, or enroll a speaker.
"enrollmentStatus": String
},
"errorInfo": {
    "errorMessage": String,
    "errorType": String,
    "errorCode": Integer
}
}

Fraudster Action

Emits events when a fraudster is successfully registered or deleted.

Events are not sent when a fraudster is associated or disassociated with a watchlist.

{"...commonfields
"detail-type": "VoiceId Fraudster Action",
"detail": {
    "sourceId": String,
    "domainID": String,
    "action": String,
    "status": String,
    "generatedFraudsterId": String,
    "watchlistIds": [String],
    "data": {
        "registrationSource": String,
        "registrationSourceId": String,
        "registrationStatus": String
    },
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}

EnrollBySession

Emits this event when an enrollment request is submitted. A Speaker event is emitted when the actual enrollment succeeds or fails.
StartSpeakerEnrollmentJob

Emits this event when a batch enrollment request is submitted, succeeds, or fails. A Speaker event is emitted for each of the individual speakers to indicate if corresponding enrollment succeeds or fails.

StartSpeakerEnrollmentJob

StartSpeakerEnrollmentJob
StartFraudsterRegistrationJob

Emits this event when a batch registration request is submitted, succeeds, or fails. A Fraudster event is emitted for each of the individual fraudsters to indicate if corresponding registration succeeds or fails.

```json
{
...commonfields
"detail-type": "VoiceId Batch Fraudster Registration Action",
"detail": {
"sourceId": String,
"domainId": String,
"action": "BATCH_REGISTRATION_REQUEST",
"status": String,
"batchJobId": String,
"data": {
"dataAccessRoleArn": String,
"registrationConfig": {
"duplicateRegistrationAction": String,
"fraudsterSimilarityThreshold": Integer,
"watchlistIds": [String],
},
"inputDataConfig": {
"s3Uri": String
},
"outputDataConfig": {
"s3Uri": String,
"kmsKeyId": String
}
}
}```
{},
"errorInfo": {
    "errorMessage": String,
    "errorType": String,
    "errorCode": Integer
}
}
Security in Amazon Connect

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon Connect, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Connect. The following topics show you how to configure Amazon Connect to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Connect resources.

Contents

- Data protection in Amazon Connect
- Identity and access management for Amazon Connect
- Logging and monitoring Amazon Connect
- Tagging resources in Amazon Connect
- Compliance validation in Amazon Connect
- Resilience in Amazon Connect
- Infrastructure security in Amazon Connect
- Cross-service confused deputy prevention
- Security Best Practices for Amazon Connect
Data protection in Amazon Connect

The AWS shared responsibility model applies to data protection in Amazon Connect. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a Name field. This includes when you work with Amazon Connect or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Contents

- Data handled by Amazon Connect
- Encryption at rest
• **Encryption in transit**

• **Key management**

• **Amazon Connect and interface VPC endpoints (AWS PrivateLink)**

## Data handled by Amazon Connect

Data held within Amazon Connect is segregated by the AWS account ID and the Amazon Connect instance ID. This ensures that data can be accessed only by the authorized users of a specific Amazon Connect instance.

Amazon Connect handles a variety of data related to the contact center, including but not limited to the following categories.

- **Resources and configurations** -- This includes queues, flows, users, routing profiles, and task templates.

- **Contact metadata** -- This includes connection time, handle time, source number (ANI), destination number (DNIS), and user defined contact attributes.

- **Agent-related performance data** -- This includes login time, status changes, and contacts handled.

- **Phone call audio streams** -- When enabled, this also includes call recordings.

- **Chat transcripts** – Included only if enabled in flows.

- **Screen recordings** – Included only if enabled in flows.

- **Attachments** – Included only if enabled at the instance level.

- **Integration configuration** – Includes user defined name, description and metadata when creating integration with external applications.

- **Knowledge documents** – This includes documents used by agents to handle contacts.

- **Voiceprints** – When Amazon Connect Voice ID is enabled, a voiceprint is created from the customer's voice for future authentication. Similarly, a voiceprint is created while registering a fraudster in the Voice ID system for future fraud detection.

- **Speaker and Fraudster Audio** – When Amazon Connect Voice ID is enabled, the audio used for enrolling speakers and registering fraudsters is stored so that Voice ID can re-enroll and reregister them in future when there is a need to do so.

- **Forecasts, capacity plans, and schedules** – Included only if enabled and created.
Amazon Connect stores the following Personally Identifiable Information (PII) data related to your customers:

- The customer's phone number: ANI for inbound calls, and DNIS for outbound calls or transfers.
- If you are using Amazon Connect Customer Profiles, all this data could potentially be PII. This data is always encrypted at rest using either a customer managed key or an AWS owned key. The Amazon Connect Customer Profiles data is segregated by the AWS account ID and the domain. Multiple Amazon Connect instances can share a single Customer Profiles domain.
- For outbound campaigns, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On the Amazon Connect side, these are always encrypted at rest using either a customer managed key or an AWS owned key. The outbound campaigns data is segregated by the Amazon Connect instance ID and are encrypted by instance-specific keys.

**External application data**

Amazon AppIntegrations enables you to integrate with external applications. It stores references to other AWS resources and client-service specified metadata. No data is stored other than incidentally while being processed. When syncing data periodically with an Amazon Connect service, data is encrypted using a customer managed key and stored temporarily for one month.

**Phone call media**

Amazon Connect is in the audio path for calls handled by the service. It is therefore responsible for relaying the call's media stream between participants. This can include the audio between a customer and a flow / IVR, the audio between a customer and an agent, or mixing the audio between multiple parties in a conference or during a transfer. There are two types of phone calls:

- PSTN calls. This includes inbound customer calls, outbound calls placed by agents to customers, and calls to an agent's physical phone, if this option has been enabled in the Contact Control Panel (CCP).
- Softphone calls placed to the agent's browser.

PSTN calls are connected between Amazon Connect and various telecommunications carriers using either private circuits maintained between Amazon Connect and our providers or existing AWS internet connectivity. For PSTN calls routed over the public internet, signaling is encrypted with TLS and the audio media is encrypted with SRTP.
Softphone calls are established to the agent's browser with an encrypted WebSocket connection using TLS. The audio media traffic to the browser is encrypted in transit using DTLS-SRTP.

**Call recordings and screen recordings**

At the instance-level, by default the call recording and screen recording capabilities are available when an Amazon S3 bucket is created for them. You determine which contacts are recorded by specifying it in the flows. This allows for more detailed control over which contacts are recorded.

Note the following behavior for call recordings:

- The call recording feature has options for choosing whether to record the agent only, customer only, or agent and customer conversations.
- A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the flow.
- When call recording is enabled, the recording begins when the call is connected to an agent and stops when the agent disconnects.
- When a customer is on hold, the agent is still recorded.
- The transfer conversation between agents is recorded.
- Any transfers to external numbers are not recorded after the agent leaves the call.
- If the agent mutes their own microphone, for example, to consult with a coworker sitting next to them, their side-bar conversation is not recorded. The customer is still recorded since their microphone hasn't been muted.

Screen recording only records the agent's screen if the contact is enabled for screen recording. Screen recording begins when the agent accepts a contact and ends with the agent completes the after contact work. Screen recording supports the voice, chat, and task channels.

You can limit access to the call and screen recordings based on user permissions. Recordings can be searched and played back within the Amazon Connect admin website.

**Call recording and screen recording storage**

Call and screen recordings are stored in two phases:

- Recordings intermediately held within Amazon Connect during and after the contact, but before delivery.
- Recordings delivered to your Amazon S3 bucket.
The recordings that are stored in your Amazon S3 bucket are secured using a KMS key that was configured when your instance was created.

At all times, you maintain full control over the security of call recordings delivered to your Amazon S3 bucket.

**Access to call recordings and screen recordings**

You can search for and listen to call recordings or view screen recordings in Amazon Connect. To determine which users can do this, assign them the appropriate permissions in their security profile. If AWS CloudTrail is enabled, access to specific recordings by Amazon Connect users is captured in CloudTrail.

The capabilities of Amazon S3, AWS KMS, and IAM put you in full control of who has access to call recording data.

**Contact metadata**

Amazon Connect stores metadata related to contacts that flow through the system and allows authorized users to access this information. The Contact Search feature allows you to search and view contact data, such as origination phone numbers or other attributes set by the flow, that are associated with a contact for diagnostics or reporting purposes.

Contact data classified as PII that is stored by Amazon Connect is encrypted at rest using a key that is time-limited and specific to the Amazon Connect instance. Specifically, the customer origination phone number is cryptographically hashed with a key that is specific to the instance to allow for use in contact search. For contact search, the encryption key is not time-sensitive.

The following data stored by Amazon Connect is treated as sensitive:

- Origination phone number
- Outbound phone number
- External numbers dialed by agents for transfers
- External numbers transferred to by a flow
- Contact name
- Contact description
- All contact attributes
- All contact references
Contact Lens real-time processing

Content processed by Contact Lens in real-time is encrypted at rest and in transit. Data is encrypted with keys owned by Contact Lens.

Voiceprints and Voice ID audio recordings

When you enable Amazon Connect Voice ID, it computes voiceprints out of your customer's speech for authenticating them in the future, and stores the data. Similarly, when you enable fraud detection, it stores the voiceprint for each fraudster registered in Voice ID.

While enrolling a customer into Voice ID for authentication and fraud detection, you must specify a CustomerSpeakerId for them. Since Voice ID stores biometric information for each speaker, we strongly recommend that you use an identifier that does not contain PII in the CustomerSpeakerId field.

Speaker and Fraudster Audio

When you enable Amazon Connect Voice ID, it stores a compacted version of the audio (called utterances) that it aggregated while enrolling a speaker or registering a fraudster. This audio is used in the future whenever the voiceprints for the speakers and fraudsters need to be regenerated. The data is retained until the speaker/fraudster is deleted. The original audio used for enrollment or evaluation is deleted after a 24 hour retention period.

The data is retained until the speaker/fraudster is deleted or opted out.

Outbound campaigns

For outbound campaigns, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On Amazon Connect, these are always encrypted at rest using either a customer managed key or an AWS owned key. The outbound campaigns data is segregated by the Amazon Connect instance ID and are encrypted by instance specific keys.

Task templates

Any processing of task template resources in Amazon Connect is encrypted at rest and in transit. Data is encrypted with an AWS KMS key.

Forecasts, Capacity Plans, and Schedules

When forecasts, capacity plans, and schedules are generated, they are always encrypted at rest and in transit. Data is encrypted with an AWS KMS key.
Encryption at rest

Contact data classified as PII, or data that represents customer content being stored by Amazon Connect, is encrypted at rest (that is, before it is put, stored, or saved to a disk) using AWS KMS encryption keys owned by AWS. For information about AWS KMS keys, see What is AWS Key Management Service? in the AWS Key Management Service Developer Guide. Contact data in non-temporary storage is encrypted such that data encryption keys generated from the KMS keys are not shared across Amazon Connect instances.

Amazon S3 server-side encryption is used to encrypt conversation recordings (voice and chat). Call recordings, screen recordings, and transcripts are stored in two phases:

• Recordings intermediately held within Amazon Connect during and after the contact, but before delivery.
• Recordings delivered to your Amazon S3 bucket.

The recordings and chat transcripts that are stored in your Amazon S3 bucket are secured using a KMS key that was configured when your instance was created.

Contents

• Amazon AppIntegrations data encryption at rest
• Amazon Connect Cases encryption at rest
• Amazon Connect Customer Profiles encryption at rest
• Amazon Q in Connect encryption at rest
• Amazon Connect Voice ID encryption at rest
• Outbound campaigns
• Forecasts, capacity plans, and schedules

Amazon AppIntegrations data encryption at rest

When you create a DataIntegration encrypted with a customer managed key, Amazon AppIntegrations creates a grant on your behalf by sending a CreateGrant request to AWS KMS. Grants in AWS KMS are used to give Amazon AppIntegrations access to a KMS key in your account.

You can revoke access to the grant, or remove the access that Amazon AppIntegrations has to the customer managed key at any time. If you do, Amazon AppIntegrations can not access any of the
data encrypted by the customer managed key, which affects operations that are dependent on that data.

External application data that Amazon AppIntegrations processes is encrypted at rest in an S3 bucket using the customer managed key that you provided during configuration. Integration configuration data is encrypted at rest using a key that is time-limited and specific to the user account.

Amazon AppIntegrations requires the grant to use the customer managed key for the following internal operations:

- Send `GenerateDataKeyRequest` to AWS KMS to generate data keys encrypted by your customer managed key.
- Send `Decrypt` requests to AWS KMS to decrypt encrypted data keys so that they can be used to encrypt your data.

**Amazon Connect Cases encryption at rest**

All customer provided data in case fields, case comments, descriptions of the fields and templates stored by Amazon Connect Cases is encrypted at rest using encryption keys stored in AWS Key Management Service (AWS KMS).

Amazon Connect Cases service owns, manages, monitors, and rotates the encryption keys (that is, AWS owned keys) to meet the high security standards. Payload of the case event streams is temporarily (typically for a few seconds) stored in Amazon EventBridge before it is made available through the default-bus in customers account. EventBridge also encrypts the entire payload at rest using AWS owned keys.

**Amazon Connect Customer Profiles encryption at rest**

All user data stored in Amazon Connect Customer Profiles is encrypted at rest. Amazon Connect Customer Profiles encryption at rest provides enhanced security by encrypting all your data at rest using encryption keys stored in AWS Key Management Service (AWS KMS). This functionality helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet strict encryption compliance and regulatory requirements.

Organizational policies, industry or government regulations, and compliance requirements often require the use of encryption at rest to increase the data security of your applications. Customer
Profiles integrated with AWS KMS to enable its encryption at rest strategy. For more information, see [AWS Key Management Service Concepts](https://docs.aws.amazon.com/kms/latest/userguide/) in the AWS Key Management Service Developer Guide.

When creating a new domain, you must provide a **KMS key** that the service will use to encrypt your data in transit and at rest. The customermanaged key is created, owned, and managed by you. You have full control over the customer managed key (AWS KMS charges apply).

You can specify an encryption key when you create a new domain or profile object type or switch the encryption keys on an existing resources by using the AWS Command Line Interface (AWS CLI), or the Amazon Connect Customer Profiles Encryption API. When you choose a customer managed key, Amazon Connect Customer Profiles creates a grant to the customer managed key that grants it access to the customer managed key.

AWS KMS charges apply for a customer managed key. For more information about pricing, see [AWS KMS pricing](https://aws.amazon.com/kms/pricing/).

**Amazon Q in Connect encryption at rest**

All user data stored in Amazon Q in Connect is encrypted at rest using encryption keys stored in AWS Key Management Service. If you optionally provide a customer managed key, Amazon Q in Connect uses it to encrypt knowledge content stored at rest outside of Amazon Q in Connect search indices. Amazon Q in Connect uses dedicated search indices per customer and they are encrypted at rest by using AWS owned keys stored in AWS Key Management Service. Additionally, you can use CloudTrail to audit any data access using the Amazon Q in Connect APIs.

AWS KMS charges apply when using a key that you provide. For more information about pricing, see [AWS KMS pricing](https://aws.amazon.com/kms/pricing/).

**Amazon Connect Voice ID encryption at rest**

Amazon Connect Voice ID stores customer voiceprints which cannot be reverse-engineered to obtain the enrolled customer's speech or identify a customer. All user data stored in Amazon Connect Voice ID is encrypted at rest. When creating a new Voice ID domain, you must provide a customer managed key that the service uses to encrypt your data at rest. The customer managed key is created, owned, and managed by you. You have full control over the key.

You can update the KMS key in the Voice ID domain by using the `update-domain` command in AWS Command Line Interface (AWS CLI), or the [UpdateDomain](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_UpdateDomain.html) Voice ID API.

When you change the KMS key, an asynchronous process will be triggered to re-encrypt the old data with the new KMS key. After this process completes, all of your domain's data will be...
encrypted under the new KMS key, and you may safely retire the old key. For more information, see UpdateDomain.

Voice ID creates a grant to the customer managed key that grants it access to the key. For more information, see How Amazon Connect Voice ID uses grants in AWS KMS.

Following is a list of data that is encrypted at rest using the customer managed key:

- **Voiceprints**: The voiceprints generated while enrolling the speakers and registering fraudsters into the system.
- **Speaker and fraudster audio**: The audio data used for enrolling the speakers and registering the fraudsters.
- **CustomerSpeakerId**: The customer-provided SpeakerId while enrolling the customer into Voice ID.
- **Customer-provided metadata**: These include free-form strings such as Domain Description, Domain Name, Job Name, and more.

AWS KMS charges apply for a customer managed key. For more information about pricing, see AWS KMS pricing.

**How Amazon Connect Voice ID uses grants in AWS KMS**

Amazon Connect Voice ID requires a grant to use your customer managed key. When you create a domain, Voice ID creates a grant on your behalf by sending a see CreateGrant request to AWS KMS. The grant is required to use your customer managed key for the following internal operations:

- Send DescribeKey requests to AWS KMS to verify that the symmetric customer managed key ID provided is valid.
- Send GenerateDataKey requests to KMS key to create data keys with which to encrypt objects.
- Send Decrypt requests to AWS KMS to decrypt the encrypted data keys so that they can be used to encrypt your data.
- Send ReEncrypt requests to AWS KMS when the key is updated to re-encrypt a limited set of data using the new key.
- Store files in S3 using the AWS KMS key to encrypt the data.

You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Voice ID won't be able to access any of the data encrypted by the
customer managed key, which affects all the operations that are dependent on that data, leading to AccessDeniedException errors and failures in the asynchronous workflows.

**Customer managed key policy for Voice ID**

Key policies control access to your customer managed key. Every customer managed key must have exactly one key policy, which contains statements that determine who can use the key and how they can use it. When you create your customer managed key, you can specify a key policy. For more information, see [Managing access to KMS keys](https://docs.aws.amazon.com/kms/latest/userguide/managed-key-control-policy.html) in the AWS Key Management Service Developer Guide.

Following is an example key policy which gives a user the permissions they need to call all Voice ID APIs using the customer managed key:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow key access to Amazon Connect VoiceID.",
      "Effect": "Allow",
      "Principal": {
        "AWS": "your_user_or_role_ARN"
      },
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": [
            "voiceid.region.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

For information about specifying permissions in a policy, see [Specifying KMS keys in IAM policy statements](https://docs.aws.amazon.com/IAM/latest/userguide/iam-policies-specifying-kms.html) in the AWS Key Management Service Developer Guide.
Voice ID encryption context

An encryption context is an optional set of key-value pairs that contain additional contextual information about the data. AWS KMS uses the encryption context as additional authenticated data to support authenticated encryption.

When you include an encryption context in a request to encrypt data, AWS KMS binds the encryption context to the encrypted data. To decrypt data, you include the same encryption context in the request.

Voice ID uses the same encryption context in all AWS KMS cryptographic operations, where the key is `aws:voiceid:domain:arn` and the value is the resource Amazon Resource Name (ARN) Amazon Resource Name (ARN).

```
"encryptionContext": {
}
```

You can also use the encryption context in audit records and logs to identify how the customer managed key is being used. The encryption context also appears in logs generated by CloudTrail or Amazon CloudWatch Logs.

Using encryption context to control access to your customer managed key

You can use the encryption context in key policies and IAM policies as conditions to control access to your symmetric customer managed key. You can also use encryption context constraints in a grant.

Amazon Connect Voice ID uses an encryption context constraint in grants to control access to the customer managed key in your account or Region. The grant constraint requires that the operations that the grant allows use the specified encryption context.

The following are example key policy statements to grant access to a customer managed key for a specific encryption context. The condition in this policy statement requires that the grants have an encryption context constraint that specifies the encryption context.

```
{
    "Condition": {
        "ArnEquality": {
        }
    }
}
```
"Sid": "Enable DescribeKey",
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
},
"Action": "kms:DescribeKey",
"Resource": "*"
},
{
  "Sid": "Enable CreateGrant",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
    }
  }
}

**Monitoring your encryption keys for Voice ID**

When you use an AWS KMS customer managed key with Voice ID, you can use [AWS CloudTrail](https://aws.amazon.com/cloudtrail) or [Amazon CloudWatch Logs](https://aws.amazon.com/cloudwatch/) to track requests that Voice ID sends to AWS KMS.

The following examples is a sample AWS CloudTrail event for `CreateGrant` operation called by Voice ID to access data encrypted by your customer managed key:

**CreateGrant**

```json
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA5STZEFPSZEOW7NP3X:SampleUser1",
    "arn": "arn:aws:sts::111122223333:assumed-role/SampleRole/SampleUser",
    "accountId": "111122223333",
    "accessKeyId": "AAAAAAA1111111EXmAMPLE",
    "sessionContext": {
```

**Encryption at rest**

2180
"sessionIssuer": {
  "type": "Role",
  "principalId": "AROA5STZEFPSZEOW7NP3X",
  "arn": "arn:aws:iam::111122223333:role/SampleRole",
  "accountId": "111122223333",
  "userName": "SampleUser"
},
"webIdFederationData": {},
"attributes": {
  "creationDate": "2021-09-14T23:02:23Z",
  "mfaAuthenticated": "false"
},
"invokedBy": "voiceid.amazonaws.com",
"eventTime": "2021-09-14T23:02:50Z",
"eventSource": "kms.amazonaws.com",
"eventName": "CreateGrant",
"awsRegion": "us-west-2",
"sourceIPAddress": "SampleIpAddress",
"userAgent": "Example Desktop/1.0 (V1; OS)",
"requestParameters": {
  "constraints": {
    "encryptionContextSubset": {
    }
  },
  "retiringPrincipal": "voiceid.amazonaws.com",
  "operations": [
    "CreateGrant",
    "Decrypt",
    "DescribeKey",
    "GenerateDataKey",
    "GenerateDataKeyPair",
    "GenerateDataKeyPairWithoutPlaintext",
    "GenerateDataKeyWithoutPlaintext",
    "ReEncryptFrom",
    "ReEncryptTo"
  ],
  "granteePrincipal": "voiceid.amazonaws.com"
},
"Encryption at rest"
DescribeKey

{  
"eventVersion": "1.08",
"userIdentity": {  
  "type": "AWSService",
  "invokedBy": "voiceid.amazonaws.com"
},
"eventTime": "2021-10-13T15:12:39Z",
"eventSource": "kms.amazonaws.com",
"eventName": "DescribeKey",
"awsRegion": "us-west-2",
"sourceIPAddress": "voiceid.amazonaws.com",
"userAgent": "voiceid.amazonaws.com",
"requestParameters": {  
  "keyId": "alias/sample-key-alias"
},
"responseElements": null,
"requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
"eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
"readOnly": true,
"resources": [{
  "accountId": "111122223333",
  "type": "AWS::KMS::Key",
  "ARN": "arn:aws:kms:us-west-2:111122223333:alias/sample-key-alias"
}]
}
"accountId": "111122223333",
"type": "AWS::KMS::Key",
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

Decrypt

{
"eventVersion": "1.08",
"userIdentity": {
  "type": "AWSService",
  "invokedBy": "voiceid.amazonaws.com"
},
"eventTime": "2021-10-12T23:59:34Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",
"awsRegion": "us-west-2",
"sourceIPAddress": "voiceid.amazonaws.com",
"userAgent": "voiceid.amazonaws.com",
"requestParameters": {
  "encryptionContext": {
    "encryptionContext": {
    }
  }
},
"encryptionAlgorithm": "SYMMETRIC_DEFAULT"
},
"responseElements": null,
"requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
"eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "encryptionContext": {
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
    }
  }
]
GenerateDataKeyWithoutPlaintext

{  
"eventVersion": "1.08",  
"userIdentity": {  
  "type": "AWSService",  
  "invokedBy": "voiceid.amazonaws.com"  
},  
"eventTime": "2021-10-13T00:26:41Z",  
"eventSource": "kms.amazonaws.com",  
"eventName": "GenerateDataKeyWithoutPlaintext",  
"awsRegion": "us-west-2",  
"sourceIPAddress": "voiceid.amazonaws.com",  
"userAgent": "voiceid.amazonaws.com",  
"requestParameters": {  
  "encryptionContext": {  
  },  
  "keySpec": "AES_256"  
},  
"responseElements": null,  
"requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",  
"eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",  
"readOnly": true,  
"resources": [{  
  "accountId": "111122223333",  
  "type": "AWS::KMS::Key",  
}]
}
ReEncrypt

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-10-13T00:59:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReEncrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "voiceid.amazonaws.com",
    "userAgent": "voiceid.amazonaws.com",
    "requestParameters": {
        "destinationEncryptionContext": {
        },
        "destinationKeyId": "arn:aws:kms:us-west-2:111122222333:key/44444444-3333-2222-1111-EXAMPLE11111",
        "sourceEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceAAD": "SampleSourceAAAD+JXBmH+ZJNM73BfHE/dwQALXp7f44VwvoJ0rLj",
        "destinationAAD": "SampleDestinationAAAD+JXBmH+ZJNM73BfHE/dwQALXp7f44VwvoJ0rLj",
        "sourceEncryptionContext": {
        },
        "destinationEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceKeyId": "arn:aws:kms:us-west-2:111122222333:key/55555555-3333-2222-1111-EXAMPLE22222"
    },
    "responseElements": null,
    "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
    "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
}
```
Outbound campaigns

For outbound campaigns, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On Amazon Connect, these are always encrypted at rest using either a customer managed key or an AWS owned key. The outbound campaigns data is segregated by the Amazon Connect instance ID and are encrypted by instance specific keys.

You can provide your own customer managed key when onboarding to outbound campaigns.

The service use this customer managed key to encrypt sensitive data at rest. The customer managed key is created, owned, and managed by you. You have full control over the customer managed key.

If you do not provide your own customer managed key, then outbound campaigns encrypts sensitive data at rest using a AWS owned key specific to your Amazon Connect instance.

AWS KMS charges apply for a customer managed key. For more information about pricing, see AWS KMS pricing.
Forecasts, capacity plans, and schedules

When you create forecasts, capacity plans, and schedules, all data are encrypted at rest using AWS owned key encryption keys stored in AWS Key Management Service.

Encryption in transit

All data exchanged with Amazon Connect is protected in transit between the user's web browser and Amazon Connect using industry-standard TLS encryption. [Which version of TLS?](#)

External data is additionally encrypted while being processed by AWS KMS.

When Amazon Connect integrates with AWS services, such as AWS Lambda, Amazon Kinesis, or Amazon Polly, data is always encrypted in transit using TLS.

When event data is forwarded from external applications to Amazon Connect it is always encrypted in transit using TLS.

Key management

You can specify AWS KMS keys, including bring your own keys (BYOK), to use for envelope encryption with Amazon S3 input/output buckets. This also applies to data used stored in Amazon Connect Customer Profiles.

Amazon Q in Connect stores knowledge documents that are encrypted at rest in S3 using a BYOK or a service-owned key. The knowledge documents are encrypted at rest in Amazon OpenSearch Service using a service-owned key. Amazon Q in Connect stores agent queries and call transcripts using a BYOK or a service-owned key.

Amazon AppIntegrations doesn't support BYOK for encryption of configuration data. When syncing external application data, periodically you are required to BYOK. Amazon AppIntegrations requires a grant to use your customer managed key. When you create a data integration, Amazon AppIntegrations sends a CreateGrant request to AWS KMS on your behalf. You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Amazon AppIntegrations won't be able to access any of the data encrypted by the customer managed key, which affects Amazon Connect services that are dependent on that data.

The knowledge documents used by Amazon Q in Connect are encrypted by an AWS KMS key.
For using Amazon Connect Voice ID, it is mandatory to provide a customer managed key KMS key (BYOK) while creating a Amazon Connect Voice ID domain, which is used to encrypt all the customer data at rest.

Outbound campaigns encrypts all sensitive data using an AWS owned key or a customer managed key. As the customer managed key is created, owned, and managed by the you, you have full control over the customer managed key (AWS KMS charges apply).

For information about AWS KMS keys see What is AWS Key Management Service? in the AWS Key Management Service Developer Guide.

Amazon Connect and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and a subset of endpoints in Amazon Connect by creating an interface VPC endpoint. Following are the supported endpoints:

- Amazon AppIntegrations
- Customer Profiles
- Outbound campaigns
- Voice ID
- Amazon Q in Connect

The core Amazon Connect service does not support AWS PrivateLink or VPC endpoints.

Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access Amazon Connect APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with the Amazon Connect APIs that integrate with AWS PrivateLink.

For more information, see the AWS PrivateLink Guide.

Creating an interface VPC endpoint for Amazon Connect

You can create an interface endpoint using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Create an interface endpoint in the AWS PrivateLink Guide.

Amazon Connect supports the following service names:

- com.amazonaws.region.app-integrations
If you enable private DNS for an interface endpoint, you can make API requests to Amazon Connect using the default DNS name for the Region. For example, voiceid.us-east-1.amazonaws.com. For more information, see DNS hostnames in the AWS PrivateLink Guide.

Creating a VPC endpoint policy

You can attach an endpoint policy to your VPC endpoint that controls access. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see Control access to services using endpoint policies in the AWS PrivateLink Guide.

Example: VPC endpoint policy

The following VPC endpoint policy grants access to the listed Amazon Connect Voice ID actions for all principals on all resources.

```json
{
    "Statement": [ 
        { 
            "Effect": "Allow",
            "Action": [ 
                "voiceid:CreateDomain",
                "voiceid:EvaluateSession",
                "voiceid:ListSpeakers"
            ],
            "Resource": "*",
            "Principal": "*
        }
    ]
}
```
Following is another example. In this one, the VPC endpoint policy grants access to the listed outbound campaigns actions for all principals on all resources.

```json
{
   "Statement"[:
      {
         "Effect":"Allow",
         "Action":
            ["connect-campaigns:CreateCampaign",
             "connect-campaigns:DeleteCampaign",
             "connect-campaigns:ListCampaigns"
            ],
         "Resource":"*",
         "Principal":"*
      }
   }
}

Identity and access management for Amazon Connect

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Amazon Connect resources. IAM is an AWS service that you can use with no additional charge.

Topics

- Audience
- Authenticating with identities
- Managing access using policies
- Required permissions for using custom IAM policies to manage access to the Amazon Connect console
- Restrict AWS resources that can be associated with Amazon Connect
- How Amazon Connect works with IAM
- Amazon Connect identity-based policy examples
- Amazon Connect resource-level policy examples
Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon Connect.

**Service user** – If you use the Amazon Connect service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Connect features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Connect, see [Troubleshooting Amazon Connect identity and access](#).

**Service administrator** – If you're in charge of Amazon Connect resources at your company, you probably have full access to Amazon Connect. It's your job to determine which Amazon Connect features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Connect, see [How Amazon Connect works with IAM](#).

**IAM administrator** – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Connect. To view example Amazon Connect identity-based policies that you can use in IAM, see [Amazon Connect identity-based policy examples](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.
You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the AWS Sign-In User Guide.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the IAM User Guide.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the AWS IAM Identity Center User Guide and Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

**AWS account root user**

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the IAM User Guide.

**Users and groups**

An IAM user is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate...
access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the IAM User Guide.

An IAM group is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named IAMAdmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the IAM User Guide.

IAM roles

An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the IAM User Guide. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the AWS IAM Identity Center User Guide.

- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.

- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.
• **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.

• **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for Amazon Connect](#) in the Service Authorization Reference. For policy details when making FAS requests, see **Forward access sessions**.

• **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the IAM User Guide.

• **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

• **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the IAM User Guide.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role (instead of a user)](#) in the IAM User Guide.
Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the IAM User Guide.

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the iam:GetRole action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the IAM User Guide.

Identity-based policies can be further categorized as inline policies or managed policies. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the IAM User Guide.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM role trust policies and Amazon S3 bucket policies. In services that support resource-based policies, service administrators can use them to control access to a specific
resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the IAM User Guide.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the IAM User Guide.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the IAM User Guide.
Required permissions for using custom IAM policies to manage access to the Amazon Connect console

If you're using custom IAM policies to manage access to the Amazon Connect console, your users need some or all of the permissions listed in this article, depending on the tasks they need to do.

⚠️ Note

Using `connect:*` in a custom IAM policy grants your users all of the Amazon Connect permissions listed in this article.

⚠️ Note

Certain pages on the Amazon Connect console, such as Tasks and Customer Profiles, require that you add permissions to your inline policies.

Contents

- AmazonConnect_FullAccess policy
- AmazonConnectReadOnlyAccess policy
- Amazon Connect console home page
- Detailed instance pages
- Overview page
- Telephony page
- Data storage page
- Data streaming page
- Flows page
- Application integration page
- Customer Profiles page
- Tasks page
- Cases page
- Amazon Q in Connect page
- Voice ID page
Amazon Connect FullAccess policy

To allow full read/write access to Amazon Connect, you must attach two policies to your users, groups, or roles. Attach the AmazonConnect_FullAccess policy and a custom policy with the following contents:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect"
        }
    ]
}
```

To allow a user to create an instance, ensure that they have the permissions granted by the AmazonConnect_FullAccess policy.

When you use AmazonConnect_FullAccess policy, note the following:

- Additional privileges are required to create a Amazon S3 bucket with a name of your choosing, or use an existing bucket while creating or updating an instance from the Amazon Connect console. If you choose default storage locations for your call recordings, chat transcripts, call transcripts, etc, they are now prefixed with "amazon-connect-".
- The aws/connect KMS key is available to use as a default encryption option. To use a custom encryption key, assign users additional KMS privileges.
- Assign users additional privileges to attach other AWS resources like Amazon Polly, Live Media Streaming, Data Streaming, and Lex bots to their Amazon Connect instances.

AmazonConnectReadOnlyAccess policy

To allow read-only access, you need to attach only the AmazonConnectReadOnlyAccess policy.
Amazon Connect console home page

The following image shows a sample Amazon Connect console home page, with an arrow pointing to the instance alias. Choose the instance alias to navigate to the detailed instance pages.

Use the permissions listed in the following table to manage access to this page.

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>List instance</td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td>Describe instance: View the details of the instance/</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td>current settings</td>
<td>connect:ListLambdaFunctions</td>
</tr>
<tr>
<td></td>
<td>connect:ListLexBots</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td></td>
<td>connect:ListApprovedOrigins</td>
</tr>
<tr>
<td></td>
<td>connect:ListSecurityKeys</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttributes</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
</tbody>
</table>

Required permissions for custom IAM policies
<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create instance</td>
<td>connect:CreateInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>ds:CheckAlias</td>
</tr>
<tr>
<td></td>
<td>ds:CreateAlias</td>
</tr>
<tr>
<td></td>
<td>ds:AuthorizeApplication</td>
</tr>
<tr>
<td></td>
<td>ds:UnauthorizeApplication</td>
</tr>
<tr>
<td></td>
<td>ds:CreateIdentityPoolDirectory</td>
</tr>
<tr>
<td></td>
<td>ds:CreateDirectory</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td></td>
<td>iam:CreateServiceLinkedRole</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
<tr>
<td></td>
<td>logs:CreateLogGroup</td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
</tr>
</tbody>
</table>

**Required permissions for custom IAM policies**

2200
<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>servicequotas:GetServiceQuota</td>
</tr>
<tr>
<td></td>
<td>profile:ListAccountIntegrations</td>
</tr>
<tr>
<td></td>
<td>profile:GetDomain</td>
</tr>
<tr>
<td></td>
<td>profile:ListDomains</td>
</tr>
<tr>
<td></td>
<td>profile:GetProfileObjectType</td>
</tr>
<tr>
<td></td>
<td>profile:ListProfileObjectTypeTemplates</td>
</tr>
<tr>
<td>Delete instance</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DeleteInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td></td>
<td>ds:DeleteDirectory</td>
</tr>
<tr>
<td></td>
<td>ds:UnauthorizeApplication</td>
</tr>
</tbody>
</table>

**Detailed instance pages**

The following image shows the navigation menu you use to access each of the detailed instance pages.
To access the detailed instance pages, you need permissions to the Amazon Connect console home page (describe/list). Or, use the **AmazonConnectReadOnlyAccess** policy.

The following tables list the granular permissions for each detailed instance page.

**Note**

To perform **Edit** actions, users also need **List** and **Describe** permissions.

### Overview page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create service-linked role</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>profile:ListAccountIntegrations</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td></td>
<td>iam:CreateServiceLinkedRole</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
</tbody>
</table>

**Telephony page**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View telephony options</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td>Enable/Disable telephony options</td>
<td>connect:UpdateInstanceAttribute</td>
</tr>
<tr>
<td>View outbound campaigns</td>
<td>connect-campaigns:GetConnectInstanceConfig</td>
</tr>
<tr>
<td></td>
<td>connect-campaigns:GetInstanceOnboardingJobStatus</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td>Enable/disable outbound campaigns</td>
<td>connect-campaigns:GetConnectInstanceConfig</td>
</tr>
<tr>
<td></td>
<td>connect-campaigns:GetInstanceOnboardingJobStatus</td>
</tr>
<tr>
<td></td>
<td>connect-campaigns:StartInstanceOnboardingJob</td>
</tr>
<tr>
<td></td>
<td>connect-campaigns:DeleteInstanceOnboardingJob</td>
</tr>
<tr>
<td></td>
<td>connect-campaigns:DeleteConnectInstanceConfig</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceAttribute</td>
</tr>
<tr>
<td></td>
<td>iam:CreateServiceLinkedRole</td>
</tr>
<tr>
<td></td>
<td>iam:DeleteServiceLinkedRole</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:DeleteRolePolicy</td>
</tr>
<tr>
<td></td>
<td>events:PutRule</td>
</tr>
<tr>
<td></td>
<td>events:PutTargets</td>
</tr>
<tr>
<td></td>
<td>events:DeleteRule</td>
</tr>
<tr>
<td></td>
<td>events:RemoveTargets</td>
</tr>
<tr>
<td></td>
<td>events:DescribeRule</td>
</tr>
<tr>
<td></td>
<td>events:ListTargetsByRule</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListKeys</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
</tbody>
</table>
# Data storage page

## Call recording section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View call recording</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit call recording</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketAcl</td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
</tbody>
</table>

## Screen recording section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View screen recording</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
</tbody>
</table>
### Action/Use case

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit screen recording</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketAcl</td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
</tbody>
</table>

### Chat transcripts section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View chat transcripts</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td>Edit chat transcripts</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>s3:ListAllMyBuckets</td>
<td></td>
</tr>
<tr>
<td>s3:GetBucketLocation</td>
<td></td>
</tr>
<tr>
<td>s3:GetBucketAcl</td>
<td></td>
</tr>
<tr>
<td>s3:CreateBucket</td>
<td></td>
</tr>
<tr>
<td>kms:CreateGrant</td>
<td></td>
</tr>
<tr>
<td>kms:DescribeKey</td>
<td></td>
</tr>
<tr>
<td>kms:ListAliases</td>
<td></td>
</tr>
<tr>
<td>kms:RetireGrant</td>
<td></td>
</tr>
</tbody>
</table>

**Attachments section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View chat attachments</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td>Edit chat attachments</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketAcl</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
</tbody>
</table>

### Live media streaming section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View live media streaming</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit live media streaming</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
</tbody>
</table>

### Exported reports section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View exported reports</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Edit exported reports</td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
</tbody>
</table>

**Data streaming page**

**Contact records section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View data streaming - Contact records</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit contact record</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>firehose:ListDeliveryStreams</td>
<td></td>
</tr>
<tr>
<td>firehose:DescribeDeliveryStream</td>
<td></td>
</tr>
<tr>
<td>kinesis:ListStreams</td>
<td></td>
</tr>
<tr>
<td>kinesis:DescribeStream</td>
<td></td>
</tr>
</tbody>
</table>

**Agent events section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View data streaming - Agent events</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfigs</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit agent events</td>
<td>connect:AssociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>kinesis:ListStreams</td>
</tr>
<tr>
<td></td>
<td>kinesis:DescribeStream</td>
</tr>
</tbody>
</table>

**Flows page**

**Flows security keys section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View flow security keys</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListSecurityKeys</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Add/remove flow security keys</td>
<td>connect:AssociateSecurityKey</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateSecurityKey</td>
</tr>
</tbody>
</table>

Lex bots section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Lex bots</td>
<td>connect:ListLexBots</td>
</tr>
<tr>
<td></td>
<td>connect:ListBots</td>
</tr>
<tr>
<td>Add/remove Lex bots</td>
<td>lex:GetBots</td>
</tr>
<tr>
<td></td>
<td>lex:GetBot</td>
</tr>
<tr>
<td></td>
<td>lex:CreateResourcePolicy</td>
</tr>
<tr>
<td></td>
<td>lex:DeleteResourcePolicy</td>
</tr>
<tr>
<td></td>
<td>lex:UpdateResourcePolicy</td>
</tr>
<tr>
<td></td>
<td>lex:DescribeBotAlias</td>
</tr>
<tr>
<td></td>
<td>lex:ListBotAliases</td>
</tr>
<tr>
<td></td>
<td>lex:ListBots</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateBot</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateBot</td>
</tr>
<tr>
<td></td>
<td>connect:ListBots</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateLexBot</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateLexBot</td>
</tr>
<tr>
<td></td>
<td>connect:ListLexBots</td>
</tr>
</tbody>
</table>
## Lambda functions section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Lambda functions</td>
<td>connect:ListLambdaFunctions</td>
</tr>
<tr>
<td>Add/remove Lambda functions</td>
<td>connect:ListLambdaFunctions connect:AssociateLambdaFunction connect:DisassociateLambdaFunction lambda:ListFunctions lambda:AddPermission lambda:RemovePermission</td>
</tr>
</tbody>
</table>

## Flow logs section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View flow log config</td>
<td>connect:DescribeInstance connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td>Enable/disable flow log</td>
<td>logs:CreateLogGroup</td>
</tr>
</tbody>
</table>

## Amazon Polly section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Amazon Polly option</td>
<td>connect:DescribeInstance connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td>Update Amazon Polly option</td>
<td>connect:UpdateInstanceAttribute</td>
</tr>
</tbody>
</table>
## Application integration page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View approved origins</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListApprovedOrigins</td>
</tr>
<tr>
<td>Edit approved origins</td>
<td>connect: AssociateApprovedOrigin</td>
</tr>
<tr>
<td></td>
<td>connect:ListApprovedOrigins</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateApprovedOrigin</td>
</tr>
</tbody>
</table>

## Customer Profiles page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View customer profiles</td>
<td>appflow:DescribeFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectorEntity</td>
</tr>
<tr>
<td></td>
<td>appflow:ListFlows</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorEntities</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorProfiles</td>
</tr>
<tr>
<td></td>
<td>cloudwatch:GetMetricData</td>
</tr>
<tr>
<td></td>
<td>kinesis:DescribeStreamSummary</td>
</tr>
<tr>
<td></td>
<td>kms:ListKeys</td>
</tr>
<tr>
<td></td>
<td>profile:GetCalculatedAttributeDefinition</td>
</tr>
<tr>
<td></td>
<td>profile:GetEventStream</td>
</tr>
<tr>
<td></td>
<td>profile:ListAccountIntegrations</td>
</tr>
<tr>
<td></td>
<td>profile:ListCalculatedAttributeDefinitions</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>profile:ListDomains</td>
</tr>
<tr>
<td></td>
<td>profile:ListEventStreams</td>
</tr>
<tr>
<td></td>
<td>sqs:ListQueues</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Edit customer profiles</td>
<td>appflow:CreateFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:CreateConnectorProfile</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DeleteFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectorEntity</td>
</tr>
<tr>
<td></td>
<td>appflow:ListFlows</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorEntities</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorProfiles</td>
</tr>
<tr>
<td></td>
<td>appflow:StartFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:StopFlow</td>
</tr>
<tr>
<td></td>
<td>kinesis:ListStreams</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:ListKeys</td>
</tr>
<tr>
<td></td>
<td>kms:ListGrants</td>
</tr>
<tr>
<td></td>
<td>profile:CreateDomain</td>
</tr>
<tr>
<td></td>
<td>profile:CreateEventStream</td>
</tr>
<tr>
<td></td>
<td>profile:DeleteEventStream</td>
</tr>
<tr>
<td></td>
<td>profile:DeleteIntegration</td>
</tr>
<tr>
<td></td>
<td>profile:DeleteDomain</td>
</tr>
<tr>
<td></td>
<td>profile:DetectProfileObjectType</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| profile:GetCalculatedAttributeDefinition
| profile:ListAccountIntegrations
| profile:ListCalculatedAttributeDefinitions
| profile:ListDomains
| profile:PutIntegration
| profile:UpdateDomain
| s3:SelectObjectContent
| sqs:ListQueues |

**Tasks page**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
| View Tasks integrations  | app-integrations:GetEventIntegration
|                          | connect:ListIntegrationAssociations                     |
| Edit Tasks integrations  | app-integrations:CreateEventIntegration
|                          | app-integrations:GetEventIntegration
|                          | app-integrations:ListEventIntegrations
|                          | app-integrations:DeleteEventIntegrationAssociation
|                          | app-integrations:CreateEventIntegrationAssociation
|                          | appflow:CreateFlow
<p>|                          | appflow:CreateConnectorProfile |</p>
<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>appflow:DescribeFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DeleteFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DeleteConnectorProfile</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectorEntity</td>
</tr>
<tr>
<td></td>
<td>appflow:ListFlows</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorEntities</td>
</tr>
<tr>
<td></td>
<td>appflow:StartFlow</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>connect:DeleteIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>connect:ListUseCases</td>
</tr>
<tr>
<td></td>
<td>connect:DeleteUseCase</td>
</tr>
<tr>
<td></td>
<td>events:ActivateEventSource</td>
</tr>
<tr>
<td></td>
<td>events:CreateEventBus</td>
</tr>
<tr>
<td></td>
<td>events:DescribeEventBus</td>
</tr>
<tr>
<td></td>
<td>events:DescribeEventSource</td>
</tr>
<tr>
<td></td>
<td>events:ListEventSources</td>
</tr>
<tr>
<td></td>
<td>events:ListTargetsByRule</td>
</tr>
<tr>
<td></td>
<td>events:PutRule</td>
</tr>
<tr>
<td></td>
<td>events:PutTargets</td>
</tr>
<tr>
<td></td>
<td>events:DeleteRule</td>
</tr>
<tr>
<td></td>
<td>events:RemoveTargets</td>
</tr>
</tbody>
</table>

Required permissions for custom IAM policies 2217
<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:ListKeys</td>
</tr>
<tr>
<td></td>
<td>kms:ListGrants</td>
</tr>
</tbody>
</table>

### Cases page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Cases domain details</td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>ds:DescribeDirectories</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>cases:GetDomain</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Onboard to Cases</td>
<td>connect:ListInstances</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>cases:GetDomain</td>
</tr>
<tr>
<td></td>
<td>cases:CreateDomain</td>
</tr>
<tr>
<td></td>
<td>connect:CreateIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
</tbody>
</table>

Required permissions for custom IAM policies
# Amazon Q in Connect page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
| View domains and integrations | wisdom:ListAssistantAssociations  
appflow:DescribeConnectorProfiles  
app-integrations:GetDataIntegration  
connect:ListIntegrationAssociations  
kms:DescribeKey  
wisdom:GetAssistant  
wisdom:GetKnowledgeBase  
wisdom:ListAssistantAssociations |
| Add or remove domains | connect:CreateIntegrationAssociation  
connect:DeleteIntegrationAssociation  
connect:ListIntegrationAssociations  
iam:DeleteRolePolicy  
iam:PutRolePolicy  
kms:CreateGrant  
kms:DescribeKey  
kms:ListAliases  
wisdom:CreateAssistant  
wisdom:DeleteAssistant  
wisdom:GetAssistant  
wisdom:ListAssistantAssociations |
<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wisdom:ListAssistants</td>
</tr>
<tr>
<td></td>
<td>wisdom:TagResource</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add or remove integrations</td>
<td>wisdom:ListAssistantAssociations</td>
</tr>
<tr>
<td></td>
<td>app-integrations:CreateDataIntegration</td>
</tr>
<tr>
<td></td>
<td>app-integrations:CreateDataIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>app-integrations:DeleteDataIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>app-integrations:GetDataIntegration</td>
</tr>
<tr>
<td></td>
<td>app-integrations:ListDataIntegrations</td>
</tr>
<tr>
<td></td>
<td>appflow:CreateConnectorProfile</td>
</tr>
<tr>
<td></td>
<td>appflow:CreateFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DeleteFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnector</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectorEntity</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectorProfiles</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeConnectors</td>
</tr>
<tr>
<td></td>
<td>appflow:DescribeFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:ListConnectorEntities</td>
</tr>
<tr>
<td></td>
<td>appflow:StartFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:StopFlow</td>
</tr>
<tr>
<td></td>
<td>appflow:TagResource</td>
</tr>
<tr>
<td></td>
<td>appflow:UseConnectorProfile</td>
</tr>
<tr>
<td></td>
<td>connect:CreateIntegrationAssociation</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>connect:DeleteIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>iam:DeleteRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:Decrypt</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:GenerateDataKey</td>
</tr>
<tr>
<td></td>
<td>kms:ListAliases</td>
</tr>
<tr>
<td></td>
<td>kms:ListGrants</td>
</tr>
<tr>
<td></td>
<td>secretsmanager:CreateSecret</td>
</tr>
<tr>
<td></td>
<td>secretsmanager:PutResourcePolicy</td>
</tr>
<tr>
<td></td>
<td>wisdom:CreateAssistantAssociation</td>
</tr>
<tr>
<td></td>
<td>wisdom:CreateKnowledgeBase</td>
</tr>
<tr>
<td></td>
<td>wisdom:DeleteAssistantAssociation</td>
</tr>
<tr>
<td></td>
<td>wisdom:DeleteKnowledgeBase</td>
</tr>
<tr>
<td></td>
<td>wisdom:GetAssistant</td>
</tr>
<tr>
<td></td>
<td>wisdom:GetKnowledgeBase</td>
</tr>
<tr>
<td></td>
<td>wisdom:ListAssistantAssociations</td>
</tr>
<tr>
<td></td>
<td>wisdom:ListKnowledgeBases</td>
</tr>
<tr>
<td></td>
<td>wisdom:TagResource</td>
</tr>
</tbody>
</table>
## Voice ID page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Voice ID integrations</td>
<td>voiceid:DescribeDomain</td>
</tr>
<tr>
<td></td>
<td>voiceid:ListDomains</td>
</tr>
<tr>
<td></td>
<td>voiceid:RegisterComplianceConsent</td>
</tr>
<tr>
<td></td>
<td>voiceid:DescribeComplianceConsent</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td>Edit Voice ID integrations</td>
<td>voiceid:DescribeDomain</td>
</tr>
<tr>
<td></td>
<td>voiceid:ListDomains</td>
</tr>
<tr>
<td></td>
<td>voiceid:RegisterComplianceConsent</td>
</tr>
<tr>
<td></td>
<td>voiceid:DescribeComplianceConsent</td>
</tr>
<tr>
<td></td>
<td>voiceid:UpdateDomain</td>
</tr>
<tr>
<td></td>
<td>voiceid:CreateDomain</td>
</tr>
<tr>
<td></td>
<td>connect:ListIntegrationAssociations</td>
</tr>
<tr>
<td></td>
<td>connect:CreateIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>connect:DeleteIntegrationAssociation</td>
</tr>
<tr>
<td></td>
<td>events:PutRule</td>
</tr>
<tr>
<td></td>
<td>events:DeleteRule</td>
</tr>
<tr>
<td></td>
<td>events:PutTargets</td>
</tr>
<tr>
<td></td>
<td>events:RemoveTargets</td>
</tr>
</tbody>
</table>
## Forecasting, capacity planning, and scheduling page

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View forecasting, capacity planning, and scheduling</td>
<td>connect:DescribeForecastingPlanningSchedulingIntegration</td>
</tr>
<tr>
<td>Enable forecasting, capacity planning, and scheduling</td>
<td>connect:UpdateInstanceAttribute connect:StartForecastingPlanningSchedulingIntegration</td>
</tr>
<tr>
<td>Disable forecasting, capacity planning, and scheduling</td>
<td>connect:UpdateInstanceAttribute connect:StopForecastingPlanningSchedulingIntegration</td>
</tr>
</tbody>
</table>

## Federations

### SAML federation

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML federation</td>
<td>connect:GetFederationToken</td>
</tr>
</tbody>
</table>

### Admin/Emergency federation

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin/Emergency federation</td>
<td>connect:GetFederationTokens</td>
</tr>
</tbody>
</table>

## Restrict AWS resources that can be associated with Amazon Connect

Each Amazon Connect instance is associated with an IAM [service-linked role](https://docs.aws.amazon.com/iam/latest/dg/slr-overview.html) when the instance is created. Amazon Connect can integrate with other AWS services for use cases such as call recording storage (Amazon S3 bucket), natural language bots (Amazon Lex bots), and data streaming.
(Amazon Kinesis Data Streams). Amazon Connect assumes the service-linked role to interact with these other services. The policy is first added to the service-linked role as part of corresponding APIs on the Amazon Connect service (that are in turn called by the AWS console). For example, if you want to use a certain Amazon S3 bucket with your Amazon Connect instance, the bucket must be passed to the `AssociateInstanceStorageConfig` API.

For the set of IAM actions defined by Amazon Connect, see [Actions defined by Amazon Connect](#).

Following are some examples of how to restrict access to other resources that may be associated with an Amazon Connect instance. They should be applied to the User or Role that is interacting with Amazon Connect APIs or the Amazon Connect console.

### Note
A policy with an explicit `Deny` would override the `Allow` policy in these examples.

For more information about what resources, condition keys, and dependent APIs you can use to restrict access, see [Actions, resources, and condition keys for Amazon Connect](#).

#### Example 1: Restrict which Amazon S3 buckets can be associated with an Amazon Connect instance

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "connect:UpdateInstanceStorageConfig",
                "connect:AssociateInstanceStorageConfig"
            ],
            "Condition": {
                "StringEquals": {
                    "connect:StorageResourceType": "CALL_RECORDINGS"
                }
            }
        }
    ],
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "connect:UpdateInstanceStorageConfig",
                "connect:AssociateInstanceStorageConfig"
            ]
        }
    ]
}
```

Restrict AWS resources that can be associated with Amazon Connect
This example allows an IAM principal to associate an Amazon S3 bucket for call recordings for the given Amazon Connect instance ARN, and a specific Amazon S3 bucket named my-connect-recording-bucket. The AttachRolePolicy and PutRolePolicy actions are scoped to the Amazon Connect service-linked role (a wildcard is used in this example, but you can provide the role ARN for the instance if needed).

Note
To use an AWS KMS key to encrypt recordings in this bucket, an additional policy is needed.

Example 2: Restrict which AWS Lambda functions can be associated with an Amazon Connect instance

AWS Lambda functions are associated with an Amazon Connect instance, but the Amazon Connect service-linked role is not used to invoke them, and so is not modified. Instead, a policy is added to the function through the `lambda:AddPermission` API that allows the given Amazon Connect instance to invoke the function.
To restrict which functions can be associated with an Amazon Connect instance, you specify the Lambda function ARN that a user can use to invoke `lambda:AddPermission`:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "connect:AssociateLambdaFunction",
        "lambda:AddPermission"
      ],
      "Resource": [
        "arn:aws:lambda:*:*:function:my-function"
      ]
    }
  ]
}
```

**Example 3: Restrict which Amazon Kinesis Data Streams can be associated with an Amazon Connect instance**

This example follows a similar model to the Amazon S3 example. It restricts which specific Kinesis Data Streams may be associated with a given Amazon Connect instance for delivering contact records.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "connect:UpdateInstanceStorageConfig",
        "connect:AssociateInstanceStorageConfig"
      ],
      "Condition": {
        "StringEquals": {
          "connect:StorageResourceType": "CONTACT_TRACE_RECORDS"
        }
      }
    }
  ]
}
```
How Amazon Connect works with IAM

Before you use IAM to manage access to Amazon Connect, you should understand what IAM features are available to use with Amazon Connect. To get a high-level view of how Amazon Connect and other AWS services work with IAM, see AWS Services That Work with IAM in the IAM User Guide.

Topics

- Amazon Connect identity-based policies
- Authorization based on Amazon Connect tags
- Amazon Connect IAM roles
Amazon Connect identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Amazon Connect supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the IAM User Guide.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as permission-only actions that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called dependent actions.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon Connect use the following prefix before the action: connect:. Policy statements must include either an Action or NotAction element. Amazon Connect defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
    "connect:action1",
    "connect:action2"
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word Describe, include the following action:

```
"Action": "connect:Describe*"
```

To see a list of Amazon Connect actions, Actions, Resources, and Condition Keys for Amazon Connect.
Resources

Amazon Connect supports resource-level permissions (specifying a resource ARN in an IAM policy). Following is a list of Amazon Connect resources:

- Instance
- Contact
- User
- Routing profile
- Security profile
- Hierarchy group
- Queue
- Flow
- Hours of operation
- Phone number
- Task templates
- Customer profile domain
- Customer profile object type
- Outbound campaigns

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as resource-level permissions.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

"Resource": "*

The Amazon Connect instance resource has the following ARN:
For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

For example, to specify the i-1234567890abcdef0 instance in your statement, use the following ARN:

"Resource": "arn:aws:connect:us-east-1:123456789012:instance/i-1234567890abcdef0"

To specify all instances that belong to a specific account, use the wildcard (*):

"Resource": "arn:aws:connect:us-east-1:123456789012:instance/*"

Some Amazon Connect actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

"Resource": "*"

Many Amazon Connect API actions involve multiple resources. For example,

To specify multiple resources in a single statement, separate the ARNs with commas.

"Resource": [
  "resource1",
  "resource2"
]

To see a list of Amazon Connect resource types and their ARNs, see Actions, Resources, and Condition Keys for Amazon Connect. The same article explains with which actions you can specify the ARN of each resource.

**Condition keys**

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Condition element (or Condition block) lets you specify conditions in which a statement is in effect. The Condition element is optional. You can create conditional expressions that use
condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple Condition elements in a statement, or multiple keys in a single Condition element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the IAM User Guide.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the IAM User Guide.

Amazon Connect defines its own set of condition keys and also supports using some global condition keys. To see all AWS global condition keys, see AWS Global Condition Context Keys in the IAM User Guide.

Example: Restricting Access to a Specific Region

To see a list of Amazon Connect condition keys, see Actions, Resources, and Condition Keys for Amazon Connect.

Examples

To view examples of Amazon Connect identity-based policies, see Amazon Connect identity-based policy examples.

Authorization based on Amazon Connect tags

You can attach tags to Amazon Connect resources or pass tags in a request to Amazon Connect. To control access based on tags, you provide tag information in the condition element of a policy using the connect:ResourceTag/key-name, aws:RequestTag/key-name, or aws:TagKeys condition keys.

To view an example identity-based policy for limiting access to a resource based on the tags on that resource, see Describe and update Amazon Connect users based on tags.
Amazon Connect IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon Connect

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Amazon Connect supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon Connect supports service-linked roles. For details about creating or managing Amazon Connect service-linked roles, see Use service-linked roles for Amazon Connect.

Choosing an IAM role in Amazon Connect

When you create a resource in Amazon Connect, you must choose a role to allow Amazon Connect to access Amazon EC2 on your behalf. If you have previously created a service role or service-linked role, then Amazon Connect provides you with a list of roles to choose from. It's important to choose a role that allows access to start and stop Amazon EC2 instances.

Amazon Connect identity-based policy examples

By default, IAM entities don't have permission to create or modify Amazon Connect resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant IAM entities permission to perform specific API operations on the specified resources they need. The IAM administrator must then attach those policies to the IAM entities that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating Policies on the JSON Tab in the IAM User Guide.

Topics
Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Connect resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see *AWS managed policies* or *AWS managed policies for job functions* in the *IAM User Guide*.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see *Policies and permissions in IAM* in the *IAM User Guide*.

- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see *IAM JSON policy elements: Condition* in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies
adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the IAM User Guide.

- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the IAM User Guide.

For more information about best practices in IAM, see Security best practices in IAM in the IAM User Guide.

**Allow IAM users to view their own permissions**

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}" ]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```
Grant "View User" permissions

When you create a user or group in your AWS account, you can associate an IAM policy with that group or user, which specifies the permissions that you want to grant.

For example, imagine you have a group of entry-level developers. You can create an IAM group named Junior application developers, and include all entry-level developers. Then, associate a policy with that group that grants them permissions to view Amazon Connect users. In this scenario, you might have a policy such as the following sample.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["connect:DescribeUser", "connect:ListUsers"],
            "Resource": "*"
        }
    ]
}
```

This sample policy grants permissions to API actions listed in the Action element.

⚠️ **Note**

If you don't specify a user ARN or ID in your statement, you must also grant the permission to use all resources for the action using the * wildcard for the Resource element.
Allow users to integrate with external applications

This example shows how you might create a policy that allows users to interact with their external application integrations.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllAppIntegrationsActions",
            "Effect": "Allow",
            "Action": [
                "app-integrations:ListEventIntegrations",
                "app-integrations:CreateEventIntegration",
                "app-integrations:GetEventIntegration",
                "app-integrations:UpdateEventIntegration",
                "app-integrations:DeleteEventIntegration",
                "app-integrations:ListDataIntegrations",
                "app-integrations:CreateDataIntegration",
                "app-integrations:GetDataIntegration",
                "app-integrations:UpdateDataIntegration",
                "app-integrations:DeleteDataIntegration"
            ],
            "Resource": "*"
        }
    ]
}
```

Describe and update Amazon Connect users based on tags

In an IAM policy, you can optionally specify conditions that control when a policy is in effect. For example, you can define a policy that allows users to update only an Amazon Connect user who is working in the test environment.

You can define some conditions that are specific to Amazon Connect, and define other conditions that apply to all of AWS. For more information and a list of AWS-wide conditions, see Condition in IAM JSON Policy Elements Reference in the IAM User Guide.

The following sample policy allows the "describe" and "update" actions for users with specific tags.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowTaggedConnectActions",
            "Effect": "Allow",
            "Action": [
                "connect:DescribeAgent",
                "connect:DescribeCapacity",
                "connect:UpdateAgent",
                "connect:UpdateCapacity"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "connect:Tag": "test"
                }
            }
        }
    ]
}
```
This policy allows "describe user" and "update user" but only for those Amazon Connect users tagged with tag "Department: Test" where "Department" is the tag key and "Test" is the tag value.

Create Amazon Connect users based on tags

The following sample policy allows the create actions for users with specific request tags.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "connect:CreateUser",
                "connect:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Owner": "TeamA"
                }
            }
        }
    ]
}
```
This policy allows "create user" and "tag resource" but the tag "Owner: TeamA" must be present in the requests.

Create and view Amazon AppIntegrations resources

The following sample policy allows event integrations to be created, listed, and fetched.

```json
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "app-integrations:CreateEventIntegration",
               "app-integrations:GetEventIntegration",
               "app-integrations::ListEventIntegrations",
           ],
           "Resource": "*"
       }
   ]
}
```

Create and view Amazon Q in Connect Assistants

The following sample policy allows Amazon Q in Connect assistants to be created, listed, fetched, and deleted.

```json
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "wisdom:CreateContent",
               "wisdom:DeleteContent",
               "wisdom:CreateKnowledgeBase",
               "wisdom:GetAssistant",
               "wisdom:GetKnowledgeBase",
               "wisdom:GetContent",
               "wisdom:GetRecommendations",
               "wisdom:GetSession",
               "wisdom:NotifyRecommendationsReceived",
           ],
           "Resource": "*"
       }
   ]
}
```
"wisdom:QueryAssistant",
"wisdom:StartContentUpload",
"wisdom:UpdateContent",
"wisdom:UntagResource",
"wisdom:TagResource",
"wisdom:CreateSession"
],
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:ResourceTag/AmazonConnectEnabled": "True"
    }
}
},
{
    "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
    ],
    "Effect": "Allow",
    "Resource": "*
}

Manage outbound campaigns resources

Onboarding permissions: The following sample policy allows Amazon Connect instances to be onboarded to outbound campaigns.

"Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
    ],
    "Resource": [
        "arn:aws:kms:region:account-id:key/key-id"
    ],
},
{
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": ["kms:Encrypt",
                "kms:GenerateDataKey", 
                "kms:GenerateDataKeyForExport",
                "kms:ReEncrypt"
            ],
    "Resource": ["arn:aws:kms:region:account-id:key/key-id"
                  ],
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    }
}
To disable outbound campaigns for an instance, add the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:RetireGrant"
            ],
            "Resource": [
            ]
        }
    ]
}
```
"arn:aws:kms:region:account-id:key/key-id"
],
},
{
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "iam:DeleteRolePolicy",
        "events:ListTargetsByRule",
        "iam:DeleteServiceLinkedRole",
        "connect-campaigns:DeleteConnectInstanceConfig"
    ],
    "Resource": "*"
}
]

Management permissions: The following sample policy allows all read and write operations on outbound campaigns.

{
    "Sid": "AllowConnectCampaignsOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:CreateCampaign",
        "connect-campaigns:DeleteCampaign",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:UpdateCampaignName",
        "connect-campaigns:GetCampaignState"
        "connect-campaigns:UpdateOutboundCallConfig",
        "connect-campaigns:UpdateDialerConfig",
        "connect-campaigns:PauseCampaign",
        "connect-campaigns:ResumeCampaign",
        "connect-campaigns:StopCampaign",
        "connect-campaigns:GetCampaignStateBatch",
        "connect-campaigns:ListCampaigns"
    ],
    "Resource": "*"
}

ReadOnly permissions: The following sample policy allows read-only access to the campaigns.
Tag-based permissions: The following sample policy restricts access to the campaigns integrated with a particular Amazon Connect instance using tags. More permissions can be added based on the use case.

```
{
    "Sid": "AllowConnectCampaignsOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:GetCampaignState"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
        }
    }
}
```

**Note**

connect-campaigns:ListCampaigns and connect-campaigns:GetCampaignStateBatch operations cannot be restricted by Tag.
Amazon Connect resource-level policy examples

Amazon Connect supports resource-level permissions for users, so you can specify actions for them for an instance, as shown in the following policies.

Contents

- Deny the "delete" and "update" actions
- Allow actions for integrations with specific names
- Allow "create users" but deny if you're assigned to a specific security profile
- Allow recording actions on a contact
- Allow or Deny queue API actions for phone numbers in a replica Region
- View specific Amazon AppIntegrations resources
- Grant access to Amazon Connect Customer Profiles
- Grant read-only access to Customer Profiles data
- Query Amazon Q in Connect only for a specific Assistant
- Grant full access to Amazon Connect Voice ID
- Grant access to Amazon Connect outbound campaigns resources

Deny the "delete" and "update" actions

This following sample policy denies the "delete" and "update" actions for users in one Amazon Connect instance. It uses a wild card at the end of the Amazon Connect user ARN so that "delete user" and "update user" are denied on the full user ARN (that is, all Amazon Connect users in the provided instance, such as arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/agent/00dtcdd1-123e-111e-93e3-11111bfbfcc1).

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "connect:DeleteUser",
                "connect:UpdateUser*
            ]
        }
    ]
}
```
Resource-level policy examples

Allow actions for integrations with specific names

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowAllAppIntegrationsActions",
         "Effect": "Allow",
         "Action": [
            "app-integrations:ListEventIntegrations",
            "app-integrations:CreateEventIntegration",
            "app-integrations:GetEventIntegration",
            "app-integrations:UpdateEventIntegration",
            "app-integrations:DeleteEventIntegration"
         ],
         "Resource": "arn:aws:appintegrations:*:*:event-integration/MyNamePrefix-*"
      }
   ]
}
```

Allow "create users" but deny if you're assigned to a specific security profile

The following sample policy allows "create users" but explicitly denies using arn:aws:connect:us-west-2:123456789012:instance/00fbeee1-123e-111e-93e3-11111bbfccc1/security-profile/11drcggg1-123e-111e-93e3-11111bbfccc17 as the parameter for security profile in CreateUser request.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "connect:CreateUser"
         ],
         "Resource": "arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bbfccc1/agent/**"
      }
   ]
}
```
Allow recording actions on a contact

The following sample policy allows "start contact recording" on a contact in a specific instance. Since contactID is dynamic, * is used.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "connect:StartContactRecording"
         ],
         "Resource": "arn:aws:connect:us-west-2:accountID:instance/instanceId/contact/*",
         "Effect": "Allow"
      }
   ]
}
```

Set up a trusted relationship with `accountID`.

The following actions are defined for the recording APIs:

- "connect:StartContactRecording"
- "connect:StopContactRecording"
- "connect:SuspendContactRecording"
- "connect:ResumeContactRecording"
Allow more contact Actions in the same role

If the same role is used to calling other contact APIs, you can list the following contact actions:

- GetContactAttributes
- ListContactFlows
- StartChatContact
- StartOutboundVoiceContact
- StopContact
- UpdateContactAttributes

Or use a wildcard to allow all contact actions, for example: "connect:*"

Allow more resources

You can also use a wildcard to allow more resources. For example, here's how to allow all connect actions on all contact resources:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": ["connect:*"],
         "Resource": "arn:aws:connect:us-west-2:accountID:instance/*/contact/*",
         "Effect": "Allow"
      }
   ]
}
```

Allow or Deny queue API actions for phone numbers in a replica Region

The [CreateQueue](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_CreateQueue.html) and [UpdateQueueOutboundCallerConfig](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_UpdateQueueOutboundCallerConfig.html) APIs contain an input field named `OutboundCallerIdNumberId`. This field represents a phone number resource that can be claimed to a traffic distribution group. It supports both the phone number V1 ARN format that is returned by [ListPhoneNumbers](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_ListPhoneNumbers.html) and the V2 ARN format that is returned by [ListPhoneNumbersV2](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/API_ListPhoneNumbersV2.html).

Following are the V1 and V2 ARN formats that `OutboundCallerIdNumberId` supports:
- **V1 ARN format**: `arn:aws:connect:your-region:your-account_id:instance/instance_id/phone-number/resource_id`
- **V2 ARN format**: `arn:aws:connect:your-region:your-account_id:phone-number/resource_id`

*Note*

We recommend using the V2 ARN format. The V1 ARN format is going to be deprecated in the future.

Provide both ARN formats for phone number resources in the replica Region

If the phone number is claimed to a traffic distribution group, to correctly allow/deny access to queue API actions for phone number resources while operating in the replica Region you must provide the phone number resource in both V1 and V2 ARN formats. If you provide the phone number resource in only one ARN format, it does not result in the correct allow/deny behavior while operating in the replica Region.

**Example 1: Deny access to CreateQueue**

For example, you're operating in the replica Region us-west-2 with account 123456789012 and instance aaaaaaaa-bbbb-cccc-dddd-0123456789012. You want to deny access to CreateQueue API when the OutboundCallerIdNumberId value is a phone number claimed to a traffic distribution group with resource ID aaaaaaaa-eeee-ffff-gggg-0123456789012. In this scenario you must use the following policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateQueueForSpecificNumber",
      "Effect": "Deny",
      "Action": "connect:CreateQueue",
      "Resource": [
      ]
    }
  ]
}
```
Where us-west-2 is the Region where the request is being made.

**Example 2: Only allow access to UpdateQueueOutboundCallerConfig**

For example, you're operating in the replica Region us-west-2 with account 123456789012 and instance aaaaaaaaa-bbbb-cccc-dddd-0123456789012. You want to only allow access to `UpdateQueueOutboundCallerConfig` API when the `OutboundCallerIdNumberId` value is a phone number claimed to a traffic distribution group with resource ID aaaaaaaaa-eeee-ffff-gggg-0123456789012. In this scenario you must use the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyAllowUpdateQueueOutboundCallerConfigForSpecificNumber",
            "Effect": "Allow",
            "Action": "connect:UpdateQueueOutboundCallerConfig",
            "Resource": [
            ]
        }
    ]
}
```

**View specific Amazon AppIntegrations resources**

The following sample policy allows a specific event integrations to be fetched.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
        }
    ]
}
```
Grant access to Amazon Connect Customer Profiles

Amazon Connect Customer Profiles use profile as the prefix for actions instead of connect. The following policy grants full access to a specific domain in Amazon Connect Customer Profiles.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "profile:*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

Set up a trusted relationship with accountID to domain domainName.

Grant read-only access to Customer Profiles data

Following is an example for granting read access to the data in Amazon Connect Customer Profiles.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "profile:SearchProfiles",
            "profile:ListObjects"
         ],
         "Effect": "Allow"
      }
   ]
}
```
Query Amazon Q in Connect only for a specific Assistant

The following sample policy allows querying only a specific Assistant.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wisdom:QueryAssistant"
            ],
            "Resource": "arn:aws:wisdom:us-west-2:accountID:assistant/assistantID"
        }
    ]
}
```

Grant full access to Amazon Connect Voice ID

Amazon Connect Voice ID uses voiceid as the prefix for actions instead of connect. The following policy grants full access to a specific domain in Amazon Connect Voice ID:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "voiceid:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Set up a trusted relationship with accountID to domain domainName.
Grant access to Amazon Connect outbound campaigns resources

Outbound campaigns uses connect-campaign as the prefix for actions instead of connect. The following policy grants full access to a specific outbound campaign.

```
{
   "Sid": "AllowConnectCampaignsOperations",
   "Effect": "Allow",
   "Action": [
      "connect-campaigns:DeleteCampaign",
      "connect-campaigns:DescribeCampaign",
      "connect-campaigns:UpdateCampaignName",
      "connect-campaigns:GetCampaignState",
      "connect-campaigns:UpdateOutboundCallConfig",
      "connect-campaigns:UpdateDialerConfig",
      "connect-campaigns:PauseCampaign",
      "connect-campaigns:ResumeCampaign",
      "connect-campaigns:StopCampaign"
   ],
}
```

AWS managed policies for Amazon Connect

To add permissions to users, groups, and roles, it is more efficient to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions that they need. To get started quickly, you can use AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the IAM User Guide.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the ReadOnlyAccess AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new
operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](https://docs.aws.amazon.com/IAM/latest/userguide/policy_comparison.html) in the *IAM User Guide*.

**AWS managed policy: AmazonConnect_FullAccess**

To allow full read/write access to Amazon Connect, you must attach two policies to your IAM users, groups, or roles. Attach the `AmazonConnect_FullAccess` policy and a custom policy with the following contents:

**Custom Policy**

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect***"
        }
    ]
}
```

**AmazonConnect_FullAccess Policy**

```json
{
    "Version": "2012-10-17",
    "Statement": [ 
        {
            "Effect": "Allow",
            "Action": [
                "connect:*",
                "ds:CreateAlias",
                "ds:AuthorizeApplication",
                "ds:CreateIdentityPoolDirectory",
                "ds:DeleteDirectory",
                "ds:DescribeDirectories",
                "ds:UnauthorizeApplication",
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams",
                "kinesis:DescribeStream",
                "kinesis:ListStreams",
            ]
        }
    ]
}
```
"kms:DescribeKey",
"kms:ListAliases",
"lex:GetBots",
"lex:ListBots",
"lex:ListBotAliases",
"logs:CreateLogGroup",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"lambda:ListFunctions",
"ds:CheckAlias",
"profile:ListAccountIntegrations",
"profile:GetDomain",
"profile:ListDomains",
"profile:GetProfileObjectType",
"profile:ListProfileObjectTypeTemplates"
],
"Resource": "*
},
{
"Effect": "Allow",
"Action": [
"profile:AddProfileKey",
"profile:CreateDomain",
"profile:CreateProfile",
"profile:DeleteDomain",
"profile:DeleteIntegration",
"profile:DeleteProfile",
"profile:DeleteProfileKey",
"profile:DeleteProfileObject",
"profile:DeleteProfileObjectType",
"profile:GetIntegration",
"profile:GetMatches",
"profile:GetProfileObjectType",
"profile:ListIntegrations",
"profile:ListProfileObjects",
"profile:ListProfileObjectTypes",
"profile:ListTagsForResource",
"profile:MergeProfiles",
"profile:PutIntegration",
"profile:PutProfileObject",
"profile:PutProfileObjectType",
"profile:SearchProfiles",
"profile:TagResource",
"profile:UntagResource",
"profile:ListProfileObjects",
"profile:ListProfileObjectTypes"
],
"Resource": "*
}
"profile:UpdateDomain",
"profile:UpdateProfile"
],
"Resource": "arn:aws:profile::*::domains/amazon-connect-*"
},
{
"Effect": "Allow",
"Action": [
    "s3:CreateBucket",
    "s3:GetBucketAcl"
],
"Resource": "arn:aws:s3:::amazon-connect-*"
},
{
"Effect": "Allow",
"Action": [
    "servicequotas:GetServiceQuota"
],
"Resource": "arn:aws:servicequotas::*::connect/*"
},
{
"Effect": "Allow",
"Action": "iam:CreateServiceLinkedRole",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "iam:AWSServiceName": "connect.amazonaws.com"
    }
}
},
{
"Effect": "Allow",
"Action": "iam:DeleteServiceLinkedRole",
"Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect*"
},
{
"Effect": "Allow",
"Action": "iam:CreateServiceLinkedRole",
"Resource": "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
"Condition": {
    "StringEquals": {
        "iam:AWSServiceName": "profile.amazonaws.com"
    }
}
},
{
"Effect": "Allow",
"Action": "iam:CreateServiceLinkedRole",
"Resource": "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
"Condition": {
    "StringEquals": {
        "iam:AWSServiceName": "profile.amazonaws.com"
    }
}
}
To allow a user to create an instance, ensure that they have the permissions granted by the AmazonConnect_FullAccess policy.

When you use AmazonConnect_FullAccess policy, note the following:

- The `iam:PutRolePolicy` allows the user who gets that policy to configure any resource in the account to work with the Amazon Connect instance. Because it grants such broad permissions, only assign it when necessary. Instead, create the service-linked role with access to the necessary resources and let the user have access to pass the service-linked role to Amazon Connect (which is granted by the AmazonConnect_FullAccess policy).

- Additional privileges are required to create an Amazon S3 bucket with a name of your choosing, or use an existing bucket while creating or updating an instance from the Amazon Connect console. If you choose default storage locations for your call recordings, chat transcripts, call transcripts, etc, they are now prefixed with "amazon-connect-".

- The `aws/connect KMS key` is available to use as a default encryption option. To use a custom encryption key, assign users additional KMS privileges.

- Assign users additional privileges to attach other AWS resources like Amazon Polly, Live Media Streaming, Data Streaming, and Lex bots to their Amazon Connect instances.

For more information and detailed permissions, see [Required permissions for using custom IAM policies to manage access to the Amazon Connect console](#).

**AWS managed policy: AmazonConnectReadOnlyAccess**

To allow read-only access, you need to attach only the AmazonConnectReadOnlyAccess policy.

**AWS managed policy: AmazonConnectServiceLinkedRolePolicy**

The AmazonConnectServiceLinkedRolePolicy role permissions policy allows Amazon Connect to complete the following actions on the specified resources. As you enable additional features in Amazon Connect, additional permissions are added for the AWSServiceRoleForAmazonConnect service-linked role to access the resources associated with those features:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConnectActions",
      "Effect": "Allow",
      "Action": [
        "connect:*"
      ],
      "Resource": ["*"]
    },
    {
      "Sid": "AllowDeleteSLR",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid": "AllowS3ObjectForConnectBucket",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::amazon-connect-*/**"]
    },
    {
      "Sid": "AllowGetBucketMetadataForConnectBucket",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ]
    }
  ]
}
[{
    "Sid": "AllowConnectLogGroupAccess",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs::*::*:log-group:/aws/connect/*/**"
    ]
},
{
    "Sid": "AllowListLexBotAccess",
    "Effect": "Allow",
    "Action": [
        "lex:ListBots",
        "lex:ListBotAliases"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowCustomerProfilesForConnectDomain",
    "Effect": "Allow",
    "Action": [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations"
    ],
    "Resource": "arn:aws:profile::*::*:domains/amazon-connect-*"
},
{
    "Sid": "AllowReadPermissionForCustomerProfileObjects",
    "Effect": "Allow",
    "Action": [
        "profile:GetProfile",
        "profile:GetProfileObject",
        "profile:GetProfileObjectAttributes",
        "profile:GetProfileObjectDefinition",
        "profile:GetProfileObjectObjectTypes",
        "profile:GetProfileObjectObjectDefinitions",
        "profile:GetProfileObjectObjectAttributes",
        "profile:GetProfileObjectObjectAttributeValues",
        "profile:GetProfileObjectVersion",
        "profile:GetProfileObjectVersionAttributes",
        "profile:GetProfileObjectVersionDefinition",
        "profile:GetProfileObjectVersionObjectTypes",
        "profile:GetProfileObjectVersionObjectDefinitions",
        "profile:GetProfileObjectVersionObjectAttributes",
        "profile:GetProfileObjectVersionObjectAttributeValues"
    ],
    "Resource": "arn:aws:profile::*::*:domains/amazon-connect-*/**"
}]
}
"Effect": "Allow",
"Action": [
   "profile:ListProfileObjects",
   "profile:GetProfileObjectType"
],
"Resource": [
   "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/"
]
},
{
   "Sid": "AllowListIntegrationForCustomerProfile",
   "Effect": "Allow",
   "Action": [
      "profile:ListAccountIntegrations"
   ],
   "Resource": "*
"},
{
   "Sid": "AllowReadForCustomerProfileObjectTemplates",
   "Effect": "Allow",
   "Action": [
      "profile:ListProfileObjectTypeTemplates",
      "profile:GetProfileObjectTypeTemplate"
   ],
   "Resource": "arn:aws:profile:*:*:/templates*"
}],
{
   "Sid": "AllowWisdomForConnectEnabledTaggedResources",
   "Effect": "Allow",
   "Action": [
      "wisdom:CreateContent",
      "wisdom:DeleteContent",
      "wisdom:CreateKnowledgeBase",
      "wisdom:GetAssistant",
      "wisdom:GetKnowledgeBase",
      "wisdom:GetContent",
      "wisdom:GetRecommendations",
      "wisdom:GetSession",
      "wisdom:NotifyRecommendationsReceived",
      "wisdom:QueryAssistant",
      "wisdom:StartContentUpload",
      "wisdom:UpdateContent",
      "wisdom:UntagResource",
      "wisdom:TagResource"}
"wisdom:CreateSession",
"wisdom:CreateQuickResponse",
"wisdom:GetQuickResponse",
"wisdom:SearchQuickResponses",
"wisdom:StartImportJob",
"wisdom:GetImportJob",
"wisdom:ListImportJobs",
"wisdom:ListQuickResponses",
"wisdom:UpdateQuickResponse",
"wisdom:DeleteQuickResponse",
"wisdom:PutFeedback"
],
"Resource": "*",
"Condition": {
    "StringEquals": {
      "aws:ResourceTag/AmazonConnectEnabled": "True"
    }
}
},
{
  "Sid": "AllowListOperationForWisdom",
  "Effect": "Allow",
  "Action": [
    "wisdom:ListAssistants",
    "wisdom:ListKnowledgeBases"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
  "Effect": "Allow",
  "Action": [
    "profile:GetCalculatedAttributeForProfile",
    "profile:CreateCalculatedAttributeDefinition",
    "profile:DeleteCalculatedAttributeDefinition",
    "profile:GetCalculatedAttributeDefinition",
    "profile:UpdateCalculatedAttributeDefinition"
  ],
  "Resource": [
    "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/**
  ]
},
{
  "Sid": "AllowPutMetricsForConnectNamespace",
  "Effect": "Allow",
  "Action": [
    "wisdom:PutFeedback"
  ],
  "Resource": "*"}
"Effect": "Allow",
"Action": "cloudwatch:PutMetricData",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "cloudwatch:namespace": "AWS/Connect"
  }
}
},
{
  "Sid": "AllowSMSVoiceOperationsForConnect",
  "Effect": "Allow",
  "Action": [
    "sms-voice:SendTextMessage",
    "sms-voice:DescribePhoneNumbers"
  ],
  "Resource": "arn:aws:sms-voice:*:*:phone-number/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
}
]
}

**AWS managed policy: AmazonConnectCampaignsServiceLinkedRolePolicy**

The AmazonConnectCampaignsServiceLinkedRolePolicy role permissions policy allows Amazon Connect outbound campaigns to complete the following actions on the specified resources.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource": "*"
    }
  ]
}
```
AWS managed policy: AmazonConnectVoiceIDFullAccess

To allow full access to Amazon Connect Voice ID, you must attach two policies to your users, groups, or roles. Attach the AmazonConnectVoiceIDFullAccess policy and the following custom policy contents to access Voice ID through the Amazon Connect console:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect"
        },
        {
            "Effect": "Allow",
            "Action": [
                "connect:CreateIntegrationAssociation",
                "connect:DeleteIntegrationAssociation",
                "connect:ListIntegrationAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:PutRule",
                "events:PutTargets",
```
The manual policy configures the following:

- The `iam:PutRolePolicy` allows the user who gets that policy to configure any resource in the account to work with the Amazon Connect instance. Because it grants such broad permissions, only assign it when necessary.

- To attach a Voice ID domain with an Amazon Connect instance, you need additional Amazon Connect and Amazon EventBridge privileges. You need privileges to call Amazon Connect APIs to create, delete, and list integration associations. You need EventBridge permissions to create and delete EventBridge rules which are used to provide contact records related to Voice ID.

Since there is no default encryption option, to use your customer managed key with your Amazon Connect Voice ID, the following API operations must be permitted in the key policy. Also, you must add these permissions on the relevant key. They are not included in the managed policy.

- `kms:Decrypt` to access or store encrypted data.
- `kms:CreateGrant` – when creating or updating a domain, used to create a grant to the customer managed key for the Voice ID domain. The grant controls access to the specified KMS key which allows access to grant operations Amazon Connect Voice ID requires. For more information about using grants, see Using grants in the AWS Key Management Service Developer Guide.
- `kms:DescribeKey` – when creating or updating a domain, allows determining the ARN for KMS key you provided.

For more about creating domains and KMS keys, see Enable Voice ID and Encryption at rest.
AWS managed policy: CustomerProfilesServiceLinkedRolePolicy

To allow Amazon Connect Customer Profiles to publish CloudWatch metrics to your AWS account, you must attach the CustomerProfilesServiceLinkedRolePolicy managed policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["cloudwatch:PutMetricData"],
         "Resource": ".",
         "Condition": {
            "StringEquals": {
               "cloudwatch:namespace": "AWS/CustomerProfiles"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": ["iam:DeleteRole"],
         "Resource": "arn:aws:iam:::role/aws-service-role/profile.amazonaws.com/AWSServiceRoleForProfile_*"
      }
   ]
}
```

AWS managed policy: AmazonConnectSynchronizationServiceRolePolicy

The AmazonConnectSynchronizationServiceRolePolicy permissions policy allows Amazon Connect Managed Synchronization to complete the following read, write, update, and delete actions on the specified resources. As resource synchronization is enabled for more resources, additional permissions are added to the AWSServiceRoleForAmazonConnectSynchronization service-linked role to access these resources.
The AmazonConnectSynchronizationServiceRolePolicy permissions policy is grouped into the following sets of permissions.

- connect – Connect permissions for the synchronization of Connect configurations and resources.
- cloudwatch – CloudWatch permissions to publish Amazon Connect usage metrics for an instance in your account.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConnectActions",
      "Effect": "Allow",
      "Action": [
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect:DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect:DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",
        "connect:CreateAgentStatus",
        "connect:UpdateAgentStatus",
        "connect:DescribeAgentStatus",
        "connect:ListAgentStatuses",
        "connect:CreateQuickConnect",
        "connect:UpdateQuickConnect*",
        "connect:DeleteQuickConnect",
        "connect:DescribeQuickConnect",
        "connect:ListQuickConnects",
        "connect:CreateHoursOfOperation",
        "connect:UpdateHoursOfOperation",
        "connect:DeleteHoursOfOperation",
        "connect:DescribeHoursOfOperation",
        "connect:ListHoursOfOperations",
        "connect:CreateQueue",
      ]
    }
  ]
}
```
"connect:UpdateQueue",
"connect:DeleteQueue",
"connect:DescribeQueue",
"connect:ListQueue",
"connect:CreatePrompt",
"connect:UpdatePrompt",
"connect:DeletePrompt",
"connect:DescribePrompt",
"connect:ListPrompts",
"connect:GetPromptFile",
"connect:CreateSecurityProfile",
"connect:UpdateSecurityProfile",
"connect:DeleteSecurityProfile",
"connect:DescribeSecurityProfile",
"connect:ListSecurityProfile",
"connect:CreateContactFlow",
"connect:UpdateContactFlow",
"connect:DeleteContactFlow",
"connect:DescribeContactFlow",
"connect:ListContactFlow",
"connect:BatchGetFlowAssociation",
"connect:CreatePredefinedAttribute",
"connect:UpdatePredefinedAttribute",
"connect:DeletePredefinedAttribute",
"connect:DescribePredefinedAttribute",
"connect:ListPredefinedAttributes",
"connect:ListTagsForResource",
"connect:TagResource",
"connect:UntagResource",
"connect:ListTrafficDistributionGroups",
"connect:ListPhoneNumbersV2",
"connect:UpdatePhoneNumber",
"connect:DescribePhoneNumber",
"connect:Associate",
"connect:Disassociate"
],
"Resource": "*
}
},
{
"Sid": "AllowPutMetricsForConnectNamespace",
"Effect": "Allow",
"Action": "cloudwatch:PutMetricData",
"Resource": "*
"Condition": {

Amazon Connect updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Connect since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Connect Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Pinpoint | Added the following actions to the service-linked role policy to use Amazon Pinpoint phone numbers to allow Amazon Connect to send SMS:  
  - `sms:DescribePhoneNumbers`  
  - `sms:SendTextMessage` | November 17, 2023 |
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Q in Connect | The following action is allowed to be performed on Amazon Q in Connect resources that have the resource tag 'AmazonConnectEnabled': 'True' on Amazon Q in Connect Knowledge Base:  
  - `wisdom:PutFeedback` | November 15, 2023 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AmazonConnectCampaignsServiceLinkedRolePolicy</strong>&lt;br&gt;– Added actions for Amazon Connect</td>
<td>Amazon Connect added new actions to retrieve outbound campaigns:&lt;br&gt;• <code>connect:BatchPutContact</code>&lt;br&gt;• <code>connect:StopContact</code></td>
<td>November 8, 2023</td>
</tr>
<tr>
<td><strong>AmazonConnectSynchronizationServiceRolePolicy</strong>&lt;br&gt;– Added new AWS managed policy</td>
<td>Added a new service-linked role managed policy for managed synchronization.&lt;br&gt;The policy provides access to read, create, update, and delete Amazon Connect resources and is used to automatically synchronize AWS resources across AWS regions.</td>
<td>November 3, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| AmazonConnectServiceLinkedRolePolicy – Added actions for Customer Profiles | Added the following action to manage Amazon Connect Customer Profiles Service Linked Roles:  
- `profile:ListCalculatedAttributesForProfile`  
- `profile:GetDomain`  
- `profile:ListIntegrations`  
- `profile:CreateCalculatedAttributeDefinition`  
- `profile:DeleteCalculatedAttributeDefinition`  
- `profile:GetCalculatedAttributeDefinition`  
- `profile:UpdateCalculatedAttributeDefinition` | October 30, 2023 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Q in Connect | The following actions are allowed to be performed on Amazon Q in Connect resources that have the resource tag 'AmazonConnectEnabled': 'True' on Amazon Q in Connect Knowledge Base:  
  - wisdom:CreateQuickResponse  
  - wisdom:GetQuickResponse  
  - wisdom:SearchQuickResponses  
  - wisdom:StartImportJob  
  - wisdom:GetImportJob  
  - wisdom:ListImportJobs  
  - wisdom:ListQuickResponses  
  - wisdom:UpdateQuickResponse  
  - wisdom:DeleteQuickResponse | October 25, 2023 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AmazonConnectServiceLinkedRolePolicy – Added</td>
<td>Added the following action to manage Amazon Connect Customer Profiles Service</td>
<td>October 6, 2023</td>
</tr>
<tr>
<td>actions for Customer Profiles</td>
<td>Linked Roles:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• profile:ListCalculatedAttributeDefinitions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• profile:GetCalculatedAttributeForProfile</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Q in Connect | The following actions are allowed to be performed on Amazon Q in Connect resources that have the resource tag 'AmazonConnectEnabled':'True' on Amazon Q in Connect knowledge bases and assistants:  
  - wisdom:CreateContent  
  - wisdom:DeleteContent  
  - wisdom:CreateKnowledgeBase  
  - wisdom:GetAssistant  
  - wisdom:GetKnowledgeBase  
  - wisdom:GetContent  
  - wisdom:GetRecommendations  
  - wisdom:GetSession  
  - wisdom:NotifyRecommendationsReceived  
  - wisdom:QueryAssistant  
  - wisdom:StartContentUpload  
  - wisdom:UntagResource  
  - wisdom:TagResource | September 29, 2023 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| • wisdom:CreateSession | The following List actions are allowed to be performed on all Amazon Q in Connect resources:  
  • wisdom:ListAssistants  
  • wisdom:KnowledgeBases | |
| **CustomerProfilesServiceLinkedRolePolicy** – Added CustomerProfilesServiceLinkedRolePolicy | New managed policy. | March 7, 2023 |
| **AmazonConnect_FullAccess** – Added permission for managing Amazon Connect Customer Profiles Service Linked Roles | Added the following action to manage Amazon Connect Customer Profiles Service Linked Roles.  
  • iam:CreateServiceLinkedRole - allows you to create a service-linked role for Customer Profiles. | January 26, 2023 |
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon CloudWatch | Added the following action to publish usage Amazon Connect metrics for an instance to your account.  
  • cloudwatch:PutMetricData | February 22, 2022 |
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **AmazonConnect_FullAccess** | Added all permissions for managing Amazon Connect Customer Profiles domains that are created for new Amazon Connect instances.  

- `profile:ListAccountIntegrations` - Lists all the integrations associated with a specific URI in the AWS account.  
- `profile:ListDomains` - Returns a list of all the domains for an AWS account that have been created.  
- `profile:GetDomain` - Returns information about a specific domain.  
- `profile:ListProfileObjectTypeTemplates` - Allow the Amazon Connect console to display a list of templates that you can use to create your data mappings.  
- `profile:GetObjectTypes` - Allow you to view all the current Object Types (data mappings) that you've created. | November 12, 2021 |

The following permissions are allowed to be performed
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>On domains with a name that is prefixed with <code>amazon-connect-</code></td>
<td>- profile:AddProfile Key   - Allows you to associate a new key value with a specific profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:CreateDomain  - Allows you to create new domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:CreateProfile  - Allows you to create new profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteDomain    - Allows you to delete domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteIntegration - Allows you to delete integrations with a domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteProfile   - Allows you to delete a profile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteProfileKey - Allows you to delete a profile key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteProfileObject - Allows you to delete a profile object</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- profile:DeleteProfileObjectType -</td>
<td>}</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Allow you to delete a profile object type</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>profile:GetIntegration</td>
<td>- Allows you to retrieve information about an integration</td>
<td></td>
</tr>
<tr>
<td>profile:GetMatches</td>
<td>- Allows you to retrieve possible profile matches</td>
<td></td>
</tr>
<tr>
<td>profile:GetProfileObjectType</td>
<td>- Allows you to retrieve profile object types</td>
<td></td>
</tr>
<tr>
<td>profile:ListIntegrations</td>
<td>- Allows you to list integrations</td>
<td></td>
</tr>
<tr>
<td>profile:ListProfileObjects</td>
<td>- Allows you to list profile objects</td>
<td></td>
</tr>
<tr>
<td>profile:ListProfileObjectTypes</td>
<td>- Allows you to list profile object types</td>
<td></td>
</tr>
<tr>
<td>profile:ListTagsForResource</td>
<td>- Allows you to list tags for a resource</td>
<td></td>
</tr>
<tr>
<td>profile:MergeProfiles</td>
<td>- Allows you to merge profile matches</td>
<td></td>
</tr>
<tr>
<td>profile:PutIntegration</td>
<td>- Allows you to add an integration between the service and a third-par</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ty service which includes Amazon AppFlow and Amazon Connect</td>
<td>• **profile:**PutProfile Object  - Allows you to create and update objects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**PutProfile ObjectType  - Allows you to create and update object types</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**SearchProfiles  - Allows you to search profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**TagResource  - Allows you to tag resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**UntagResource  - Allows you to untag resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**UpdateDomain  - Allows you to update domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• **profile:**UpdateProfile  - Allows you to update profiles</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Connect Customer Profiles | Added the following actions so Amazon Connect flows and the agent experience can interact with the profiles in your default Customer Profiles domain:  
  - profile:SearchProfiles  
  - profile:CreateProfile  
  - profile:UpdateProfile  
  - profile:AddProfileKey | November 12, 2021 |

Added the following action so Amazon Connect flows and the agent experience can interact with the profile objects in your default Customer Profiles domain:

- profile:ListProfileObjects

Added the following action so Amazon Connect flows and the agent experience can determine whether Customer Profiles is enabled for your Amazon Connect instance:
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>• profile:ListAccountIntegrations</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AmazonConnectVoiceIDFullAccess</strong> – Added new AWS managed policy</td>
<td>Added a new AWS managed policy so you can set up your users to use Amazon Connect Voice ID. This policy provides full access to Amazon Connect Voice ID through the AWS console, SDK, or other means.</td>
<td>September 27, 2021</td>
</tr>
<tr>
<td><strong>AmazonConnectCampaignsServiceLinkedRolePolicy</strong> – Added new service-linked role policy</td>
<td>Added a new service-linked role policy for outbound campaigns. The policy provides access to retrieve all the outbound campaigns.</td>
<td>September 27, 2021</td>
</tr>
</tbody>
</table>
| **AmazonConnectServiceLinkedRolePolicy** – Added actions for Amazon Lex | Added the following actions for the all bots created in the account across all Regions. These actions were added to support integration with Amazon Lex.  
  • lex:ListBots - Lists all the bots available in a given Region for your account.  
  • lex:ListBotAliases - Lists all the aliases for a given bot. | June 15, 2021          |
### Change Description

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **AmazonConnect_FullAccess** – Added actions for Amazon Lex | Added the following actions for all bots created in the account across all Regions. These actions were added to support integration with Amazon Lex.  
- `lex:ListBots`  
- `lex:ListBotAliases` | June 15, 2021 |
| Amazon Connect started tracking changes | Amazon Connect started tracking changes for its AWS managed policies. | June 15, 2021 |

### Troubleshooting Amazon Connect identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Connect and IAM.

**Topics**

- [I am not authorized to perform iam:PassRole](#)
- [I want to allow people outside of my AWS account to access my Amazon Connect resources](#)

### I am not authorized to perform iam:PassRole

If you receive an error that you’re not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Connect.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user namedmarymajor tries to use the console to perform an action in Amazon Connect. However, the action requires the service to have
permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

User: arn:aws:iam::123456789012:user/marvymajor is not authorized to perform: iam:PassRole

In this case, Mary's policies must be updated to allow her to perform the iam:PassRole action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

**I want to allow people outside of my AWS account to access my Amazon Connect resources**

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Connect supports these features, see [How Amazon Connect works with IAM](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the IAM User Guide.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the IAM User Guide.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users (identity federation)](#) in the IAM User Guide.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the IAM User Guide.

**Use service-linked roles for Amazon Connect**

**What are service-linked roles (SLR) and why are they important?**

Amazon Connect uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to an Amazon Connect instance.
Service-linked roles are predefined by Amazon Connect and include all the permissions that Amazon Connect requires to call other AWS services on your behalf.

You need to enable service-linked roles so you can use new features in Amazon Connect, such as tagging support, the new user interface in User management and Routing profiles, and queues with CloudTrail support.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

**Service-linked role permissions for Amazon Connect**

Amazon Connect uses the service-linked role with the prefix **AWSServiceRoleForAmazonConnect_<unique-id>** – Grants Amazon Connect permission to access AWS resources on your behalf.

The AWSServiceRoleForAmazonConnect prefixed service-linked role trusts the following services to assume the role:

- connect.amazonaws.com

The [AmazonConnectServiceLinkedRolePolicy](#) role permissions policy allows Amazon Connect to complete the following actions on the specified resources:

- Action: all Amazon Connect actions, connect:*, on all Amazon Connect resources.
- Action: IAM iam:DeleteRole to allow deletion of the service-linked role.
- Action: Amazon S3 s3:GetObject, s3:DeleteObject, s3:GetBucketLocation, and s3:GetBucketAcl for the S3 bucket specified for recorded conversations.
  
  It also grants s3:PutObject, s3:PutObjectAcl, and s3:GetObjectAcl to the bucket specified for exported reports.
- Action: Amazon Lex lex:ListBots, lex:ListBotAliases for all bots created in the account across all Regions.
- Action: Amazon Connect Customer Profiles
  
  - profile:SearchProfiles
• profile:CreateProfile
• profile:UpdateProfile
• profile:AddProfileKey
• profile:ListProfileObjects
• profile:ListAccountIntegrations
• profile:ListProfileObjectTypeTemplates
• profile:GetProfileObjectTypeTemplate
• profile:ListProfileObjectTypes
• profile:GetProfileObjectType
• profile:ListCalculatedAttributeDefinitions
• profile:GetCalculatedAttributeForProfile
• profile:ListCalculatedAttributesForProfile
• profile:GetDomain
• profile:ListIntegrations
• profile:CreateCalculatedAttributeDefinition
• profile:DeleteCalculatedAttributeDefinition
• profile:GetCalculatedAttributeDefinition
• profile:UpdateCalculatedAttributeDefinition

to use your default Customer Profiles domain (including profiles and all object-types in domain) with the Amazon Connect flows and agent experience applications.

• Action: Amazon Connect Amazon Q in Connect
  • wisdom:CreateContent
  • wisdom:DeleteContent
  • wisdom:CreateKnowledgeBase
  • wisdom:GetAssistant
  • wisdom:GetKnowledgeBase
  • wisdom:GetContent
  • wisdom:GetRecommendations
  • wisdom:GetSession
  • wisdom:NotifyRecommendationsReceived
• wisdom:QueryAssistant
• wisdom:StartContentUpload
• wisdom:UntagResource
• wisdom:TagResource
• wisdom:CreateSession
• wisdom:CreateQuickResponse
• wisdom:GetQuickResponse
• wisdom:SearchQuickResponses
• wisdom:StartImportJob
• wisdom:GetImportJob
• wisdom:ListImportJobs
• wisdom:ListQuickResponses
• wisdom:UpdateQuickResponse
• wisdom:DeleteQuickResponse
• wisdom:PutFeedback

with resource tag 'AmazonConnectEnabled': 'True' on all Amazon Connect Amazon Q in Connect resources associated with your Amazon Connect instance.

• wisdom:ListAssistants
• wisdom:KnowledgeBases

on all Amazon Connect Amazon Q in Connect resources.

• Action: Amazon CloudWatch Metrics cloudwatch:PutMetricData to publish Amazon Connect usage metrics for an instance to your account.

• Action: Amazon Pinpoint sms:DescribePhoneNumbers and sms:SendTextMessage to allow Amazon Connect to send SMS.

As you enable additional features in Amazon Connect, the following permissions are added for the service-linked role to access the resources associated with those features by using in-line policies:

• Action: Amazon Kinesis Data Firehose firehose:DescribeDeliveryStream and firehose:PutRecord, and firehose:PutRecordBatch for the delivery stream defined for agent event streams and contact records.
- **Action:** Amazon Kinesis Data Streams `kinesis:PutRecord`, `kinesis:PutRecords`, and `kinesis:DescribeStream` for the stream specified for agent event streams and contact records.

- **Action:** Amazon Lex `lex:PostContent` for the bots added to your instance.

- **Action:** Amazon Connect Voice-ID `voiceid:*` for the Voice ID domains associated with your instance.

- **Action:** EventBridge `events:PutRule` and `events:PutTargets` for the Amazon Connect managed EventBridge rule for publishing CTR records for your associated Voice ID domains.

- **Action:** outbound campaigns
  - `connect-campaigns:CreateCampaign`
  - `connect-campaigns:DeleteCampaign`
  - `connect-campaigns:DescribeCampaign`
  - `connect-campaigns:UpdateCampaignName`
  - `connect-campaigns:GetCampaignState`
  - `connect-campaigns:GetCampaignStateBatch`
  - `connect-campaigns:ListCampaigns`
  - `connect-campaigns:UpdateOutboundCallConfig`
  - `connect-campaigns:UpdateDialerConfig`
  - `connect-campaigns:PauseCampaign`
  - `connect-campaigns:ResumeCampaign`
  - `connect-campaigns:StopCampaign`

  for all operations related to outbound campaigns.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the *IAM User Guide*.

### Create a service-linked role for Amazon Connect

You don't need to manually create a service-linked role. When you create a new instance in Amazon Connect in the AWS Management Console, Amazon Connect creates the service-linked role for you.
If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new instance in Amazon Connect, Amazon Connect creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role with the Amazon Connect - Full access use case. In the IAM CLI or the IAM API, create a service-linked role with the connect.amazonaws.com service name. For more information, see Creating a service-linked role in the IAM User Guide. If you delete this service-linked role, you can use this same process to create the role again.

**For instances created before October 2018**

If your Amazon Connect instance was created before October 2018, you don't have service-linked roles set up. To create a service-linked role, on the Account overview page, choose Create service-linked role, as shown in the following image.

For a list of the IAM permissions required to create the service-linked role, see Overview page in the Required permissions for using custom IAM policies to manage access to the Amazon Connect console topic.

**Edit a service-linked role for Amazon Connect**

Amazon Connect does not allow you to edit the AWSServiceRoleForAmazonConnect prefixed service-linked role. After you create a service-linked role, you cannot change the name of the role.
because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

Checking a service-linked role has permissions for Amazon Lex

1. On the navigation pane of the IAM console, choose Roles.
2. Choose the name of the role to modify.

Delete a service-linked role for Amazon Connect

You don't need to manually delete the AWSServiceRoleForAmazonConnect prefixed role. When you delete your Amazon Connect instance in the AWS Management Console, Amazon Connect cleans up the resources and deletes the service-linked role for you.

Supported Regions for Amazon Connect service-linked roles

Amazon Connect supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.

Use service-linked roles for outbound campaigns

Amazon Connect outbound campaigns uses AWS Identity and Access Management service-linked roles. When an Amazon Connect instance is enabled to use outbound campaigns, it creates a unique service linked role that allows it to perform actions on the Amazon Connect instance.

A service-linked role makes setting up outbound campaigns easier because you don't have to manually add the necessary permissions. Outbound campaigns defines the permissions of its service-linked roles, and unless defined otherwise, only outbound campaigns can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS services that work with IAM in the IAM User Guide. Look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for outbound campaigns

Outbound campaigns uses the service-linked role prefixed AWSServiceRoleForConnectCampaigns—Grants outbound campaigns permission to access AWS resources on your behalf.
The AWSServiceRoleForConnectCampaigns service-linked role trusts the following services to assume the role:

- connect-campaigns.amazonaws.com

The AmazonConnectCampaignsServiceLinkedRolePolicy role permissions policy allows outbound campaigns to complete the following actions on the specified resources. Additional permissions are added for the service-linked role to access the resources:

- Action: Outbound campaigns connect-campaigns:ListCampaigns for the AWS account.
- Action: Amazon Connect connect:BatchPutContact and connect:StopContact for all Amazon Connect instances.
- Action: Amazon Connect connect:StartOutboundVoiceContact connect:GetMetricData and connect:GetCurrentMetricData for the Amazon Connect instance specified.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Create a service-linked role for outbound campaigns

You don’t need to manually create a service-linked role. When you associate an Amazon Connect instance with outbound campaigns by invoking the StartInstanceOnboardingJob API, outbound campaigns creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you associate a new Amazon Connect instance with outbound campaigns, Amazon Connect creates the service-linked role for you again.

Edit a service-linked role for outbound campaigns

Outbound campaigns does not allow you to edit the AWSServiceRoleForConnectCampaigns service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.
Delete a service-linked role for outbound campaigns

If you no longer need outbound campaigns, we recommend that you delete the associated service-linked role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

To delete outbound campaigns resources used by the AWSServiceRoleForConnectCampaigns

- Delete all campaigns setup for the AWS account.

To manually delete the service-linked role using IAM

- Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForConnectCampaigns service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.

Supported Regions for outbound campaigns service-linked roles

Outbound campaigns supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

Using service-linked roles for Amazon AppIntegrations

Amazon AppIntegrations uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon AppIntegrations. Service-linked roles are predefined by Amazon AppIntegrations and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon AppIntegrations easier because you don’t have to manually add the necessary permissions. Amazon AppIntegrations defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon AppIntegrations can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon AppIntegrations resources because you can’t inadvertently remove permission to access the resources.
For information about other services that support service-linked roles, see [AWS Services That Work with IAM](#) and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

**Service-linked role permissions for Amazon AppIntegrations**

Amazon AppIntegrations uses the service-linked role named **AWSServiceRoleForAppIntegrations** which allows AppIntegrations to access AWS services and resources on your behalf.

The AWSServiceRoleForAppIntegrations service-linked role trusts the following service to assume the role:

- `app-integrations.amazonaws.com`

The role permissions policy named `AppIntegrationsServiceLinkedRolePolicy` allows Amazon AppIntegrations to complete the following actions on the specified resources:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "cloudwatch:PutMetricData"
         ],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "cloudwatch:namespace": "AWS/AppIntegrations"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": [
            "appflow:DescribeConnectorEntity",
            "appflow:ListConnectorEntities"
         ],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "appflow:namespace": "AWS/AppIntegrations"
            }
         }
      }
   ]
}
```
"Effect": "Allow",
"Action": [
   "appflow:DescribeConnectorProfiles",
   "appflow:UseConnectorProfile"
],
"Resource": "arn:aws:appflow:*::*:connector-profile/*"
},
{
"Effect": "Allow",
"Action": [
   "appflow:DeleteFlow",
   "appflow:DescribeFlow",
   "appflow:DescribeFlowExecutionRecords",
   "appflow:StartFlow",
   "appflow:StopFlow",
   "appflow:UpdateFlow"
],
"Condition": {
   "StringEquals": {
      "aws:ResourceTag/AppIntegrationsManaged": "true"
   }
},
"Resource": "arn:aws:appflow:*::*:flow/FlowCreatedByAppIntegrations-*"
},
{
"Effect": "Allow",
"Action": [
   "appflow:TagResource"
],
"Condition": {
   "ForAllValues:StringEquals": {
      "aws:TagKeys": [
         "AppIntegrationsManaged"
      ]
   }
},
"Resource": "arn:aws:appflow:*::*:flow/FlowCreatedByAppIntegrations-*"
]
• Action: `cloudwatch:PutMetricData` on "*" using the `StringEquals` condition "cloudwatch:namespace": "AWS/AppIntegrations".

• Action: `appflow:DescribeConnectorEntity` and `appflow:ListConnectorEntities` on "*".

• Action: `appflow:DescribeConnectorProfiles` and `appflow:UseConnectorProfile` on arn:aws:appflow::*:*:connector-profile/*


• Action: `appflow:TagResource` on arn:aws:appflow::*:*:flow/FlowCreatedByAppIntegrations-* using the `ForAllValues:StringEquals` condition AppIntegrationsManaged.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating a service-linked role for Amazon AppIntegrations

You don't need to manually create a service-linked role. When you create a data or event integration using either the Amazon Q in Connect, Customer Profiles, or Tasks widget in Amazon Connect in the AWS Management Console, the AWS CLI, or the AWS API, Amazon AppIntegrations creates the service-linked role for you.

⚠️ Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, if you created any new Amazon AppIntegrations resources after September 30, 2022, when it began supporting service-linked roles, then Amazon AppIntegrations created the AWSServiceRoleForAppIntegrations role in your account. To learn more, see A new role appeared in my IAM account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a data or event integration using
either the Amazon Q in Connect, Customer Profiles, or Tasks widget in Amazon Connect, Amazon AppIntegrations creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role with the AppIntegrations use case. In the AWS CLI or the AWS API, create a service-linked role with the app-integrations.amazonaws.com service name. For more information, see Creating a service-linked role in the IAM User Guide. If you delete this service-linked role, you can use this same process to create the role again.

### Editing a service-linked role for Amazon AppIntegrations

Amazon AppIntegrations does not allow you to edit the AWSServiceRoleForAppIntegrations service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

### Deleting a service-linked role for Amazon AppIntegrations

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it. You must first delete your data and event integration associations in the AWS Console and then delete your data and event integrations using the AWS CLI.

1. Go to the Amazon Q in Connect section of the Amazon Connect Console and choose the name of the data integration association that you wish to delete.
2. Choose Delete on the right hand side of the Integration details section.
3. In the pop-box, enter the name of the integration for confirmation and choose Delete.
To delete data integrations used by the AWSServiceRoleForAppIntegrations using the AWS CLI

1. List your data integrations in order to view the names of your existing integrations.
   
   `aws appintegrations list-data-integrations`

2. Delete each integration using the data integration name.
   
   `aws appintegrations delete-data-integration --data-integration-identifier DATA_INTEGRATION_NAME`

To delete event integration associations used by the AWSServiceRoleForAppIntegrations in the AWS Console

1. Go to the Customer Profiles or the Tasks section of the Amazon Connect Console and choose the name of the event integration association that you wish to delete.

2. Once you choose an event integration on the Tasks section, a pop-up will appear. Choose the Remove connection button and enter the word remove to delete your event integration association.

To delete event integrations used by the AWSServiceRoleForAppIntegrations using the AWS CLI

1. List your event integrations in order to view the names of your existing integrations.
   
   `aws appintegrations list-event-integrations`

2. Delete each integration using the data integration name.
   
   `aws appintegrations delete-event-integration --name EVENT_INTEGRATION_NAME`

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAppIntegrations service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.
Supported regions for Amazon AppIntegrations service-linked roles

Amazon AppIntegrations supports using service-linked roles in all of the regions where the service is available. For more information, see AWS regions and endpoints.

You can use the AWSServiceRoleForAppIntegrations role in the following regions.

<table>
<thead>
<tr>
<th>Region name</th>
<th>Region identity</th>
<th>Support in Amazon AppIntegrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>Yes</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Using service-linked roles for Amazon Connect Customer Profiles

Amazon Connect Customer Profiles uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Customer Profiles. Service-linked roles are predefined by Customer Profiles and include all the permissions that the service requires to call other AWS services on your behalf.
A service-linked role makes setting up Amazon Connect Customer Profiles easier because you don't have to manually add the necessary permissions. Amazon Connect Customer Profiles defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Connect Customer Profiles can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see [AWS services that work with IAM](#) and look for the services that have Yes in the Service-linked roles column. Choose a Yes with a link to view the service-linked role documentation for that service.

**Service-linked role permissions for Amazon Connect Customer Profiles**

Amazon Connect Customer Profiles uses the service-linked role named `AWSServiceRoleForProfile_unique-id` which allows Amazon Connect Customer Profiles to access AWS services and resources on your behalf.

The `AWSServiceRoleForProfile` prefixed service-linked role trusts the following services to assume the role:

- profile.amazonaws.com

The role permissions policy named CustomerProfilesServiceLinkedRolePolicy allows Amazon Connect Customer Profiles to complete the following actions on the specified resources:

- Action: Amazon CloudWatch Metrics `cloudwatch:PutMetricData` to publish Amazon Connect usage metrics for an instance to your account.
- Action: IAM `iam:DeleteRole` to delete the `AWSServiceRoleForProfile` prefixed service-linked role itself when associated Amazon Connect Customer Profiles Domain is deleted.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the [IAM User Guide](#).

**Creating a service-linked role for Amazon Connect Customer Profiles**

You don't need to manually create a service-linked role. When you create your first Amazon Connect Customer Profiles Domain in the AWS Management Console, the AWS CLI, or the AWS API, Customer Profiles creates the service-linked role for you. Note each Amazon Connect Customer
Profiles domain requires a dedicated SLR in order for Amazon Connect Customer Profiles to take actions for you.

⚠️ **Important**

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. Also, if you were using the Amazon Connect Customer Profiles service before June 8, 2023, when it began supporting service-linked roles, then Amazon Connect Customer Profiles created the **AWSServiceRoleForProfile** prefixed role in your account. To learn more, see [A new role appeared in my IAM account](#).

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create your first Amazon Connect Customer Profiles Domain, Customer Profiles creates the service-linked role for you again.

### Editing a service-linked role for Amazon Connect Customer Profiles

Amazon Connect Customer Profiles does not allow you to edit the **AWSServiceRoleForProfile** prefixed service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the [IAM User Guide](#).

### Deleting a service-linked role for Amazon Connect Customer Profiles

You don't need to manually delete the **AWSServiceRoleForProfile** prefixed role. When you delete the Amazon Connect Customer Profiles Domain in the AWS Management Console, the AWS CLI, or the AWS API, Customer Profiles cleans up the resources and deletes the service-linked role for you.

You can also use the AWS CLI or the AWS API to manually delete the service-linked role. To do this, you must first manually clean up the resources for your service-linked role and then you can manually delete it.

⚠️ **Note**

If the Amazon Connect Customer Profiles service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.
To delete Amazon Connect Customer Profiles resources used by the AWSServiceRoleForProfile prefixed service-linked role

- Delete the Amazon Connect Customer Profiles domain in the AWS Management Console, the AWS CLI, or the AWS API.

To manually delete the service-linked role using IAM

Use the AWS CLI or the AWS API to delete the AWSServiceRoleForProfile prefixed service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.

Supported regions for Amazon Connect Customer Profiles service-linked roles

Amazon Connect Customer Profiles supports using service-linked roles in all of the regions where the service is available. For more information, see AWS regions and endpoints.

<table>
<thead>
<tr>
<th>Region name</th>
<th>Region identity</th>
<th>Support in Amazon Connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>Yes</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>ap-northeast-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
<td>Yes</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
<td>Yes</td>
</tr>
<tr>
<td>Africa (Cape Town)</td>
<td>af-south-1</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Using service-linked roles for Amazon Connect Managed Synchronization

Amazon Connect managed synchronization uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Managed Synchronization. Service-linked roles are predefined by Managed Synchronization and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Managed Synchronization easier because you don't have to manually add the necessary permissions. Managed Synchronization defines the permissions of its service-linked roles, and unless defined otherwise, only Managed Synchronization can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Managed Synchronization resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have Yes in the Service-linked roles column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Managed Synchronization

Managed Synchronization uses the service-linked role that is prefixed with AWSServiceRoleForAmazonConnectSynchronization which grants Amazon Connect Managed Synchronization read, write, update, and delete permission to access AWS resources on your behalf. The full name of the role in your account will contain the prefix and a unique ID that will be similar to the following:

AWSServiceRoleForAmazonConnectSynchronization_unique-id

The AWSServiceRoleForAmazonConnectSynchronization prefixed service-linked role trusts the following services to assume the role:

- synchronization.connect.amazonaws.com

The role permissions policy named AmazonConnectSynchronizationServiceRolePolicy allows Managed Synchronization to complete the following actions on the specified resources:
• Action: Amazon Connect for all Amazon Connect resources
  • connect:DescribeUser*
  • connect:ListUser*
  • connect:CreateUser*
  • connect:DeleteUser*
  • connect:UpdateUser*
  • connect:Associate*
  • connect:Disassociate*
  • connect:DescribePredefinedAttribute
  • connect:ListPredefinedAttributes
  • connect:CreatePredefinedAttribute
  • connect:DeletePredefinedAttribute
  • connect:UpdatePredefinedAttribute
  • connect:BatchGetFlowAssociation
  • connect:DescribePhoneNumber
  • connect:UpdatePhoneNumber
  • connect:ListPhoneNumbersV2
  • connect:ListTrafficDistributionGroups
  • connect:DescribeRoutingProfile
  • connect:ListRoutingProfile*
  • connect:CreateRoutingProfile
  • connect:DeleteRoutingProfile
  • connect:UpdateRoutingProfile*
  • connect:CreateAgentStatus
  • connect:DescribeAgentStatus
  • connect:ListAgentStatuses
  • connect:UpdateAgentStatus
  • connect:CreateQuickConnect
  • connect:DeleteQuickConnect
  • connect:DescribeQuickConnect
• `connect:ListQuickConnects`
• `connect:UpdateQuickConnect*`
• `connect:CreateHoursOfOperation`
• `connect:DeleteHoursOfOperation`
• `connect:DescribeHoursOfOperation`
• `connect:ListHoursOfOperations`
• `connect:UpdateHoursOfOperation`
• `connect:DescribeQueue`
• `connect:ListQueue*`
• `connect:CreateQueue`
• `connect:DeleteQueue`
• `connect:UpdateQueue*`
• `connect:CreatePrompt`
• `connect:ListPrompts`
• `connect:UpdatePrompt`
• `connect:DeletePrompt`
• `connect:DescribePrompt`
• `connect:GetPromptFile`
• `connect:CreateSecurityProfile`
• `connect:DeleteSecurityProfile`
• `connect:DescribeSecurityProfile`
• `connect:ListSecurityProfile*`
• `connect:UpdateSecurityProfile`
• `connect:CreateContactFlow*`
• `connect:DeleteContactFlow*`
• `connect:DescribeContactFlow*`
• `connect:ListContactFlow*`
• `connect:UpdateContactFlow*`
• connect:UntagResource
• Action: Amazon CloudWatch metrics cloudwatch:PutMetricData to publish Amazon Connect usage metrics for an instance to your account.

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

Creating a service-linked role for Managed Synchronization

You don't need to manually create a service-linked role. When you replicate an Amazon Connect instance by invoking the ReplicateInstance API, Managed Synchronization creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you replicate the Amazon Connect instance again, Managed Synchronization creates the service-linked role for you again.

Editing a service-linked role for Managed Synchronization

Managed Synchronization does not allow you to edit the AWSServiceRoleForAmazonConnectSynchronization prefixed service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

Deleting a service-linked role for Managed Synchronization

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don’t have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note

If the Managed Synchronization service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.
To delete Managed Synchronization resources used by the AWSServiceRoleForAmazonConnectSynchronization prefixed role

- Delete all replica Amazon Connect instances for the source instance.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonConnectSynchronization prefixed service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.

Supported Regions for Managed Synchronization service-linked roles

Managed Synchronization supports using service-linked roles in all of the Regions where Amazon Connect Global Resiliency is available. For more information, see Set up Amazon Connect Global Resiliency.

<table>
<thead>
<tr>
<th>Region name</th>
<th>Region identity</th>
<th>Support in Managed Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>Yes</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Logging and monitoring Amazon Connect

Monitoring is important for maintaining the reliability, availability, and performance of your contact center.

You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multipoint failure if one occurs. But before you start monitoring Amazon Connect, you should create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What data about your Amazon Connect instance will you monitor?
- How often will you monitor your instance?
- What monitoring tools will you use?
• Who will perform the monitoring tasks?
• Who should be notified when something goes wrong?

See the following topics to learn how to use Amazon CloudWatch Logs and AWS CloudTrail to monitor Amazon Connect and describes the Amazon Connect metrics sent to CloudWatch:

• Monitoring your instance using CloudWatch
• Logging Amazon Connect API calls with AWS CloudTrail

Tagging resources in Amazon Connect

A *tag* is a custom metadata label that you can add to a resource in order to make it easier to identify, organize, and find in a search. Tags are comprised of two individual parts: A tag key and a tag value. This is referred to as a key:value pair.

A *tag key* typically represents a larger category, while a tag value represents a subset of that category. For example you could have tag key=Color and tag value=Blue, which would produce the key:value pair Color:Blue. Note that you can set the value of a tag to an empty string, but you can't set the value of a tag to null. Omitting the tag value is the same as using an empty string.

Tag keys can be up to 128 characters in length and tag values can be up to 256 characters in length; both are case sensitive. For more information, see:

• Amazon Connect TagResource
• Amazon Connect Customer Profiles TagResource
• Amazon Connect Voice ID TagResource: You can add tags to the Voice ID domain.
• Amazon AppIntegrations TagResource

Amazon Connect services support up to 50 tags per resource. For a given resource, each tag key must be unique with only one value.
**Note**

Your tags cannot begin with `aws:` because AWS reserves this prefix for system-generated tags. You cannot add, modify, or delete `aws:*` tags, and they don't count against your tags-per-resource limit.

The following table describes the Amazon Connect resources that can be tagged using the AWS CLI or an AWS SDK.

**Tagging support for Amazon Connect resources**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Supports tagging using the Amazon Connect console</th>
<th>Supports tagging using the CLI/SDK</th>
<th>Supports tagging on creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent group</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent group level</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent state</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Contact</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Contact evaluations</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Evaluation forms</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Flow</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flow module</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Instance</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Integration association</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Outbound campaign</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource</td>
<td>Supports tagging using the Amazon Connect console</td>
<td>Supports tagging using the CLI/SDK</td>
<td>Supports tagging on creation</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
<td>----------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Operating hours</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Phone number</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prompt</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue agent</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Queues</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quick connects</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Routing Profile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security profile</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Task template</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic distribution group</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transfer destination</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Use case</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vocabulary</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To learn more about tagging, including best practices, see Tagging AWS resources in the AWS General Reference.

**Tag-based access control**

To use tags to control access to resources within your AWS accounts, you need to provide tag information in the condition element of an IAM policy. For example, to control access to your Voice ID domain based on the tags you've assigned to it, use the `aws:ResourceTag/key-name`
condition key to specify which tag key:value pair must be attached to the domain, in order to allow given actions for it.

For more detailed information on tag-based access control in the Amazon Connect console, see Tag-based access control.

For more detailed information on tag-based access control in IAM, see Controlling access to AWS resources using tags in the IAM User Guide

Compliance validation in Amazon Connect

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.

- **Architecting for HIPAA Security and Compliance on Amazon Web Services** – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

Note
Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.

- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.

- **AWS Customer Compliance Guides** – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of
Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).

- **Evaluating Resources with Rules** in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.

- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see *Security Hub controls reference*.

- **AWS Audit Manager** – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

### Best practices for PII compliance in Amazon Connect

Following this list of best practices can help you ensure your Amazon Connect contact center is PII (Personally Identifiable Information) compliant.

- Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.

- AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.

- Use encryption in the **Store customer input** block for sensitive DTMF information.

- Use your own KMS key when ingesting data in Amazon Connect Customer Profile domains.

- Do not upload content containing customer PII to Amazon Q in Connect.

- When using Amazon Connect Voice ID, do not use PII in the `CustomerSpeakerId`.

- As with any AWS service, we strongly recommend that you not use sensitive information to name resources.

### Best practices for PCI compliance in Amazon Connect

Following this list of best practices can help you ensure your Amazon Connect contact center is PCI-compliant.
• Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.

• Payment card information (PCI) should be collected using encrypted DTMF.

• If PCI is captured in call recordings, the PCI data must be scrubbed from the recording and obfuscated from any logs or transcriptions. We recommend working with an Amazon Solution Architect if you need help doing this.

• Use encryption in transit and at rest for any downstream integration points.

• Enable multi-factor authentication (MFA) for any access to PCI as Amazon Connect is a public endpoint.

• For a detailed walkthrough that explains how to encrypt PCI, see Creating a secure IVR solution with Amazon Connect.

• AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.

• Use encryption in the Store customer input block for sensitive DTMF information.

• Use your own KMS key when ingesting data in Amazon Connect Customer Profile domains.

• For more information, see https://www.pcisecuritystandards.org.

Best practices for HIPAA compliance in Amazon Connect

Following this list of best practices can help you ensure your Amazon Connect contact center is HIPAA compliant.

• Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.

• AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.

• Use encryption in the Store customer input block for sensitive DTMF information.

• Do not upload content subject to HIPAA to Amazon Q in Connect.

• For more information about HIPAA compliance, see https://www.hipaacompliance.org/.
Resilience in Amazon Connect

The AWS global infrastructure is built around AWS Regions and Availability Zones (AZs). AWS Regions provide multiple physically separated and isolated AZs, which are connected with low-latency, high-throughput, and highly redundant networking. These AZs are physically separated by many miles, but still close enough together (60 miles or less) to be used as a single logical data center.

Each AZ features one or more discrete data centers, each housed in its own facility with redundant power, networking, and connectivity. These measures act as safeguards, and minimize the likelihood of an issue like a power outage or earthquake impacting multiple data centers or multiple AZs.

AZs are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](https://aws.amazon.com/global-infrastructure/).

Amazon Connect runs on AWS proven infrastructure operating in multiple AZs within various geographic regions around the world. This makes Amazon Connect more highly available, fault tolerant, and scalable than would be possible if a contact center solution was run from a single data center.

Within each AWS Region you can create an Amazon Connect instance, with a minimum of 3 AZs. When you create an Amazon Connect instance, that instance is propagated across those AZs in an active-active-active configuration. If there is a failure in one AZ, that node is taken out of rotation without impacting production. This architecture allows you to perform maintenance, release new features, and expand infrastructure without requiring any downtime.

**Single-region telephony and softphone architecture**

Amazon Connect is integrated with multiple telephony providers with redundant dedicated network paths to three or more AZs in every AWS Region where the service is offered today. If a particular component, data center, or an entire AZ experiences failure, the affected endpoint is automatically taken out of rotation. This allows you to continue providing a consistent quality experience for your customers.

Inbound (US toll-free) and outbound calls in Amazon Connect are processed through multiple telecom carriers. Each carrier is connected to multiple AZs in an active-active configuration. This ensures that impairment of a network path or an entire AZ does not impact your end-customer experience.
experience. It also ensures that inbound US toll-free and outbound calls will be placed through multiple carriers so impairment at the carrier level doesn't impact your customer's experience.

The following diagram illustrates this process:

1. Callers reach your contact center using carriers that operate across multiple AZs at all times.
2. RespOrg routes US toll-free traffic across multiple carriers in an active-active fashion.
3. Outbound calling is load balanced across multiple telephony providers.
4. An agent's browser chooses from at least two servers across multiple AZs, based on reachability.

More resources

To learn more about resiliency for Amazon Connect, the following resources from AWS Workshop Studio are highly recommended:

- Amazon Connect Global Resiliency Best Practices
- Amazon Connect Global Resiliency and AWS Services Multi-Region Best Practices

Infrastructure security in Amazon Connect

As a managed service, Amazon Connect is protected by the AWS global network security procedures that are described on the Best Practices for Security, Identity, and Compliance page.

You use AWS published API calls to access Amazon Connect through the network.

Supported versions of TLS

Clients must support Transport Layer Security (TLS) 1.2 or later.
Amazon Connect offers a new website access model with a new domain (instance name.my.connect.aws) that supports TLS 1.2 or newer versions only. It is available by default for instances created after March 2021. Existing customers can opt in to using the new domain using the following methods:

- For non-SAML Amazon Connect instances, change your access URL from .awsapps.com/connect to .my.connect.aws and log in again.
- For SAML-enabled instances, specify an extra query parameter new_domain=true in the relay state URL and log in again. For more information, see Use a destination in your relay state URL.

**Other requirements**

Clients must support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

You can call these API operations from any network location, but Amazon Connect does support resource-based access policies, which can include restrictions based on the source IP address.

**Cross-service confused deputy prevention**

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the calling service) calls another service (the called service). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the aws:SourceArn and aws:SourceAccount global condition context keys in resource policies to limit the permissions that Amazon Connect gives another service to the resource. If you use both global condition context keys, the aws:SourceAccount value and the
account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The most effective way to protect against the confused deputy problem is to use the exact Amazon Resource Name (ARN) of the resource you want to allow. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (*) for the unknown portions of the ARN. For example, `arn:aws:service-name::region-name::your AWS account ID:*`.

**Amazon Connect Customer Profiles cross-service confused deputy prevention**

The following examples show policies that apply to cases where someone else is set up as the administrator for Amazon Connect Customer Profiles. Use these policies to prevent the confused deputy problem.

**Example Amazon Connect Customer Profiles policy to create Customer Profile domains**

```json
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "ConfusedDeputyPreventionExamplePolicy",
        "Effect": "Allow",
        "Principal": {
            "Service": "profile.amazonaws.com"
        },
        "Action": ["kms:GenerateDataKey", "kms:CreateGrant", "kms:Decrypt"],
        "Resource": [
            "arn:aws:kms:your region-name:your AWS account ID:key/your key ARN"
        ],
        "Condition": {
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:profile:your region name:your AWS account ID:domains/your Customer Profiles domain name"
            },
            "StringEquals": {
                "aws:SourceAccount": "your AWS account ID"
            }
        }
    }
}
```
Example Amazon Connect Customer Profiles policy to create Customer Profiles object types

```json
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "ConfusedDeputyPreventionExamplePolicy",
        "Effect": "Allow",
        "Principal": {
            "Service": "profile.amazonaws.com"
        },
        "Action": ["kms:GenerateDataKey", "kms:CreateGrant", "kms:Decrypt"],
        "Resource": [
            "arn:aws:kms:
            your Region:
            your AWS account ID:key/your key ARN"
        ],
        "Condition": {
            " ArnEquals": {
                "aws:SourceArn": "arn:aws:profile:
                your region name:
                your AWS account ID:domains/
                your Customer Profiles domain name/objects/
                your object type"
            },
            "StringEquals": {"aws:SourceAccount": "your AWS account ID"
            }
        }
    }
}
```

Example Amazon Connect Customer Profiles policy to create and update dead-letter queues

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Amazon Connect Customer Profiles to publish messages to your queue",
            "Effect": "Allow",
            "Principal": {
                "Service": "profile.amazonaws.com"
            },
            "Action": "sqs:SendMessage",
            "Resource": "your dead-letter queue ARN",
            "Condition": {
                "StringEquals": {
                    "StringEquals": {
```
Example Amazon Connect Customer Profiles policy to protect the Amazon S3 bucket used as part of the Identity Resolution process

```
{
  "Sid": "Allow Amazon Connect Customer Profiles to put S3 objects to your bucket",
  "Effect": "Allow",
  "Principal": {
    "Service": "profile.amazonaws.com"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::your S3 bucket name/*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "your AWS account ID"
    },
    "ArnEquals": {
      "aws:SourceArn": "arn:aws:profile:your region name:your AWS account ID:domains/*"
    }
  }
}
```

Amazon Connect Voice ID cross-service confused deputy prevention

The following Voice ID example shows a resource policy to apply to prevent the confused deputy problem.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      
```
Amazon Connect chat message streaming cross-service confused deputy prevention

The following Amazon Connect example shows a resource policy to apply to prevent the confused deputy problem.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":{
                "Service":"connect.amazonaws.com"
            },
            "Action":"sns:Publish",
            "Resource":"your SNS topic ARN",
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":"your AWS account ID"
                },
                "ArnEquals":{
                    "aws:SourceArn":"your Amazon Connect instance ARN"
                }
            }
        }
    ]
}
```
Security Best Practices for Amazon Connect

Amazon Connect provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

Contents

- Amazon Connect Preventative Security Best Practices
- Amazon Connect Detective Security Best Practices

Amazon Connect Preventative Security Best Practices

- Ensure that all profile permissions are as restrictive as possible. Allow access to only those resources absolutely required for the user's role. For example, don't give agents permissions to create, read, or update users in Amazon Connect.

- Ensure that multi-factor authentication (MFA) is set up through your SAML 2.0 identity provider, or Radius server, if that's more applicable for your use case. After MFA is set up, a third text box becomes visible on the Amazon Connect login page to provide the second factor.

- If you use an existing directory through AWS Directory Service or SAML-based authentication for identity management, ensure that you follow all security requirements appropriate for your use case.

- Use the Log in for emergency access URL on the instance page of the AWS console only in emergency situations, not for daily use. For more information, see Emergency admin login.

Use Service Control Policies (SCPs)

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to users and roles in the affected accounts. You can use SCPs to protect critical resources associated with your Amazon Connect workload.

Set a Service Control Policy to prevent the deletion critical resources

If you're using SAML 2.0-based authentication and delete the AWS IAM Role that is used for authenticating Amazon Connect users, users won't be able to login to the Amazon Connect
instance. You will need to delete and recreate users to be associated with a new Role. This results in the deletion of all data associated with those users.

To prevent the accidental deletion of critical resources and to protect the availability of your Amazon Connect instance, you can set a [Service Control Policy (SCP)](https://docs.aws.amazon.com/service-authorization/latest/sca/policiesSample.html) as an additional control.

Following is an example SCP that can be applied at the AWS Account, Organizational Unit, or Organizational Root to prevent the deletion of the Amazon Connect instance and associated Role:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonConnectRoleDenyDeletion",
      "Effect": "Deny",
      "Action": ["iam:DeleteRole"],
      "Resource": ["arn:aws:iam::*:role/Apartment Connect user role"]
    },
    {
      "Sid": "AmazonConnectInstanceDenyDeletion",
      "Effect": "Deny",
      "Action": ["connect:DeleteInstance"],
      "Resource": ["Amazon Connect instance ARN"]
    }
  ]
}
```

**Amazon Connect Detective Security Best Practices**

Logging and monitoring are important for the availability, reliability and, performance of contact center. You should log relevant information from Amazon Connect flows to CloudWatch and build alerts and notifications based on the same.
Define log retention requirements and lifecycle policies early on, and plan to move log files to cost-efficient storage locations as soon as practical. Amazon Connect public APIs log to CloudTrail. Review and automate actions based on CloudTrail logs.

We recommend Amazon S3 for long-term retention and archiving of log data, especially for organizations with compliance programs that require log data to be auditable in its native format. Once log data is in an Amazon S3 bucket, define lifecycle rules to automatically enforce retention policies and move these objects to other, cost-effective storage classes, such as Amazon S3 Standard - Infrequent Access (Standard - IA) or Amazon S3 Glacier.

The AWS Cloud provides flexible infrastructure and tools to support both sophisticated partner offerings and self-managed centralized-logging solutions. This includes solutions such as Amazon OpenSearch Service and Amazon CloudWatch Logs.

You can implement fraud detection and prevention for incoming contacts by customizing Amazon Connect flows per your requirements. For example, you can check incoming contacts against previous contact activity in Dynamo DB and then take actions such as disconnecting a contact who is on a deny list.
Agent training guide for the CCP and agent workspace

Agent workspace

With the agent workspace you can access all Amazon Connect features in a single application. You can:

- Use the Contact Control Panel (CCP) to interact with customer contacts.
- Use Customer Profiles to view customer information.
- Use Cases to create, edit, and resolve customer cases.
- Use Amazon Q in Connect to obtain the information you need from your company knowledge base.

To access the agent workspace use the following URL:

- https://instance name.my.connect.aws/agent-app-v2/

Where instance name is provided by your IT department or the individuals that set up Amazon Connect for your business.

The following image shows the agent workspace with the CCP, Customer Profiles, Cases, and Amazon Q in Connect.
1. Set your status.
2. Access to the number pad, quick connects, and task creation.
3. Log in and out. Set your language preferences, device settings (if enabled), and phone type.
4. Inbox of inbound calls, chats, and tasks.
5. Based on the channel of the contact that is in focus in your inbox, the appropriate content shows here; for example, when a chat is selected, the chat interface appears.
6. View customer information for the contact that is in focus in your inbox.
7. Search and view cases.
8. Search for knowledge articles to solve customer issues.

CCP

You use the Amazon Connect Contact Control Panel (CCP) to interact with customer contacts. It's how you receive calls, chat with contacts, transfer them to other agents, put them on hold, and perform other key tasks.
The URL to launch the CCP is:

- https://instance name.my.connect.aws/ccp-v2/

Where instance name is provided by your IT department or the individuals that set up Amazon Connect for your business.

Large businesses often choose to customize their CCP. For example, they might want to integrate it with a CRM. However, this section describes how CCP works before it is customized.

The following image shows the CCP.

1. Set your status.
2. The channels enabled for your agent routing profile.
3. Log in and out. Set your language preferences, device settings (if enabled), and phone type.
4. Name of the agent that's currently signed in.
5. Choose a predefined destination to transfer the contact. Or call an external number.
6. Call a number or enter digits into an IVR menu.

Training video: How to use the CCP

The following video introduces you to the Contact Control Panel (CCP). It shows how to perform common tasks, such as login and setup, accept incoming calls, place calls, transfer calls, accept chat, and more.

Amazon Connect

Launch the CCP

The URL to launch the CCP is:

- https://instance name.my.connect.aws/ccp-v2/

Where instance name is provided by your IT department or whoever set up Amazon Connect for your business. The following image shows an example URL for the CCP.

With this updated CCP, your agents can manage voice, chat, and tasks from this single interface.
As the administrator, you can also launch the CCP directly from the Amazon Connect console. Just choose the phone icon in the upper right corner.

To provide agents the ability to launch the CCP from their desktop and start handling contacts, there are a few things you need to do:

- Add agents as users to the instance. For more information, see Manage users in Amazon Connect.
- Configure permissions for the agents. By default, agents assigned to the Agent security profile can access the CCP and make outbound calls. But you can create a custom security profile and add additional permissions. For more information, see Security profiles.
- Give agents the URL the CCP.
- Provide agents with their user name and password so that they can log in to the CCP.

We recommend telling agents to bookmark the URL to the CCP for more convenient access.

Agents can use the CCP with a softphone on their computer, or a deskphone. If they're using a softphone, they must use Chrome, Edge, or Firefox for their web browser. For more information, see Grant microphone access in Chrome, Firefox, or Edge.

Log in and log out of the Amazon Connect CCP

Before you can log in to the Contact Control Panel (CCP), your administrator must give you the following information:

- The URL to launch the CCP:
  - https://instance name.my.connect.aws/ccp-v2/

  Where instance name is provided by your IT department or whoever set up Amazon Connect for your business.
- Your agent ID.
- Your agent password.

To log in

After you have that information, here's how to log in and get started.

1. Ensure that your USB headset is securely connected to your computer.
2. Using Chrome or Firefox, open the CCP by using the URL that you received from your administrator.

3. Enter your agent ID and password, and then choose **Sign In**.

4. If you're prompted to **Allow access to cookies**, choose **Grant access**, and then choose **Allow**.
Amazon Connect uses cookies for authentication. Google Chrome requires you to authorize the use of Amazon Connect cookies.

**Tip**

*IT admins*: For more information, see [Use Amazon Connect Streams API for third-party cookies](#).

5. If you are prompted to allow access to your microphone and speaker, choose **Allow**.

You're all set to go!

**Problems logging in?**

If you have problems logging in to the CCP, contact your manager for help, or the IT Department for your organization.

**Log out of the Amazon Connect CCP**

**Important**

Closing the CCP doesn't automatically sign out an agent. Amazon Connect still tries to route contacts to them. To change this behavior, a developer can customize CCP for your contact center. For instructions, see [CCPv1: Log out agents automatically when they close their CCP](#).
1. At the top of the CCP, choose **Settings**.
2. Choose **Log out**.

**Using the CCP: Allow access to cookies**

When logging into the CCP you may see one of these banners:

![Banner](https://mytest98.awsapps.com)

**Action required!**

**Allow access to cookies**

The Amazon Connect Contact Control Panel (CCP) now requires permissions to access your Amazon Connect login cookies. Choose the Grant access button and use the Allow option. [Learn more](https://mytest98.awsapps.com)
Amazon Connect uses cookies for authentication. Google Chrome requires you to authorize the use of Amazon Connect cookies.

1. When you log in to the CCP, on the Allow access to cookies banner choose Grant access.
2. At the next prompt, choose Allow.

You may need to repeat these steps periodically, for example, if your organization requires it every 30 days.

**What happens if you don't choose Grant access when prompted?**

If you don't choose Grant access when prompted, you won't be able to log into the CCP. To enable access outside of the login workflow, perform the following steps:

1. Navigate to chrome://settings/content/storageAccess.
2. In the left navigation menu, choose Privacy and security.
3. Choose Third-party cookies.
4. Under You blocked these sites from using info they've saved about you, delete any entries associated with awsapps.com or connect.aws as shown in the following image.
5. You can close that instance of your browser.

6. Open your CCP. When prompted, choose **Grant access**, and then choose **Allow**.

**How to use the CCP or agent workspace to change your audio device settings**

When you're using the CCP or agent workspace, you can choose your preferred device for the audio, microphone, and ringer. This allows you to have audio notifications to ring from a desktop/laptop speaker instead of a headset, for example.
Tip

- **IT admins**: Agents need **Contact Control Panel (CCP) - Audio device settings** permissions in their security profile to access this feature.

- **Developers**: If you are embedding the CCP into a CRM or custom desktop, you can use either the **Audio device settings** security profile permission or [Amazon Connect Streams](https://aws.amazon.com/connect_streams) to pass the enableAudioDeviceSettings parameter to enable audio device settings upon initialization. If either of those flags is true, the audio device settings user interface is displayed in **Settings** on the CCP.

  For granular permission, we recommend using the security profile permission. The Streams flag is supported for backward compatibility.

---

**Change audio device settings in the CCP**

1. In the CCP or agent workspace, choose **Settings**. The **Settings** dialog box appears, similar to the following image.
2. Under **Audio devices**, use the dropdown to select your **Speaker**, **Microphone**, and **Ringer**.

**Prerequisite: Allow your browser to access your microphone**

Before you can change your audio device settings in the CCP, you need to make sure you've given your browser permission to access your microphone. This populates the device list in the CCP.

If you haven't done this yet, see the instructions for your browser.

- [Chrome](#)
- [Edge](#)
- [Firefox](#)

**Firefox limitations**

If you use Firefox for your browser, you can change only your microphone setting using the CCP. You can't change speaker and ringer settings in CCP due to a limitation with this browser. With your
operating system's sound device settings you can change your device for audio output, however, both speaker and ringer audio will come from the same device. We recommend using another supported browser for this feature.

**What to check when your audio device isn't working as expected**

Following are the top tips for resolving issues with audio devices.

- Check that your headset is properly connected to your desktop.
- Ensure that Windows exclusive mode is not enabled. For instructions, see [How do I turn off Exclusive-Mode for a Windows audio playback device?](#)
- Ensure that the device is not muted or disabled in your operating system settings. Following are instructions for a Windows computer:
  1. Press **Windows + I** to open **Settings**.
  2. Click **System**, and then click **Sound** on the left navigation pane.
  3. Scroll down the page and click **Microphone privacy settings**.
  4. Under **Allow apps to access your microphone**, set the toggle to **On**.

**Forward calls to a mobile device (iPhone, Android)**

You can take the audio portion of a call on your mobile device, and at the same time use your computer to access the Contact Control Panel. This topic explains how to forward calls to your mobile device.

1. In your Contact Control Panel (CCP), open Settings.
2. Under **Phone type**, choose **Desk phone**.
3. Enter the phone number for your mobile device, and choose **Save**.
When a contact calls, the audio portion of the call goes to your mobile device. At the same time, on your computer you can manage the call using the CCP.

**View your schedule in the agent workspace**

If your organization uses the forecasting, capacity planning, and scheduling features of Amazon Connect you can view your schedule in the agent workspace, the Contact Control Panel (CCPv1 or CCPv2), the Salesforce CTI, or a custom-built agent desktop.

Following are steps you use to view your schedule in the agent workspace.

1. Log on to the agent workspace using the URL that your admin gives you (for example, `https://[instance name].my.connect.aws/ccp-v2/`).
2. Choose the Calendar icon on the application navigation bar to launch the staff schedule manager viewer. Otherwise, the staff schedule manager viewer launches automatically.

   The following image shows a sample schedule in the agent workspace.
You can see a daily or weekly view of your schedule.

**Set your status to "Available" in the CCP**

When an agent is ready to handle calls or chats, they need to set their status in the CCP to **Available**. This tells Amazon Connect they are ready to handle contacts.

Amazon Connect uses information in the agent's [routing profile](#) to determine which contacts to route to them.

For more information about agent statuses, see [About agent status](#). For information about how Amazon Connect counts the Available status in the real-time metrics report, see [Available](#).

**Set your "Next status" in the CCP**

**Note**

"Next status" is available only to customers who are using the latest Contact Control Panel (CCP). The URL for the latest CCP ends with `ccp-v2`. 
Use the **Next status** feature to pause new contacts being routed to you, while you finish your current contacts. When all your slots are cleared, Amazon Connect automatically sets your CCP to the next status, such as **Lunch**.

The following images of the Contact Control Panel (CCP) show how to use this feature.

1. Available: The agent is on a contact.
2. The agent chooses their next status, such as **Lunch**. They can choose only a custom (**NPT**) status, or **Offline**.
3. The agent is in **Next status: Lunch**. They are still on contact. No new contacts can be routed to them.
4. The contact ends. The agent finishes ACW, and chooses **Clear contact**. Instead of going back to **Available**, their CCP is automatically set to **Lunch**.

### How to cancel "Next status"

You can easily switch from **Next status** back to **Available**. The ability to switch your status is useful, for example, if you accidentally choose **Next status: Lunch**, or if you decide not to go to **Lunch** before Amazon Connect automatically sets to that status.

The following images show this workflow.
1. While working on the same contact, the agent cancels **Next status: Lunch** and goes back to **Available**.

2. The contact ends and the agent is still **Available** for new contacts to be routed to them.

**Example 1: Set "Next status" while handling only ACW contacts**

Let's say an agent is finishing after contact work (ACW) for one or more contacts, such as a voice contact or multiple chats. They are not on contact with anyone.

Instead of choosing **Clear contact** when the agent finishes ACW, they choose **Lunch**. This puts them in **Next status: Lunch** only briefly.

Here's what happens in this scenario:

1. Agent finishes ACW and chooses **Lunch** instead of **Clear contact**.

2. Amazon Connect stops routing new contacts to them.
3. All their slots are cleared. This is so the agent doesn't have to choose `Clear contact` to end the ACW.

4. Because all the ACWs have been cleared, Amazon Connect immediately starts the automatic transition that sets the agent's status to **Lunch**.

   Agents were put into **Next status - Lunch** only briefly (milliseconds!). They might even see it in the CCP if they look fast enough.

This order of events mirrors how the CCP works when agents change their status while working on ACW. For example, an agent is finishing ACW and they set their status to **Lunch**. Here's what happens next:

1. Amazon Connect stops routing new contacts to them.
2. The ACW slot is cleared for the agent so they don't have to choose `Clear contact`.
3. The agent is set to **Lunch**.

**Example 2: Set "Next status" while managing some chats on contact and other chats in ACW**

Let's say an agent is managing two chats:

- Customer 1 is in ACW.
- Customer 2 is on contact.

While still on a contact, the agent sets their status to **Offline**. This puts them in the **Next status: Offline** state.

Here's what happens in this scenario:

1. The agent sets their status to **Offline**.
2. Amazon Connect stops routing new contacts to them.
3. The contact that is in ACW is cleared so the agent doesn't have to choose `Clear contact`. Only the connected chat remains.
4. The agent's status is **Next status: Offline**, and they continue working on their connected chat.
5. After they finish work on that contact, the agent chooses `Clear contact` to end the ACW.
6. Amazon Connect automatically sets the agent's status to **Offline**.

## Work with calls in the CCP

The topics in this section explain how to use the Amazon Connect Contact Control Panel to manage customer calls.

### Contents

- How to use the CCP to accept incoming calls
- Transfer calls to a quick connect or external phone number
- Multi-party calls: Add additional participants to an ongoing call
- How to use the CCP to make outbound calls
- View a call transcript during ACW

### How to use the CCP to accept incoming calls

1. Whenever you set your status in the CCP to **Available**, Amazon Connect can deliver calls to you, based on the settings in your **routing profile**.

2. When a call arrives, choose the **Accept call** button.
3. Before you're connected to the contact, Amazon Connect announces the name of the originating queue.

4. You're now talking to the contact.

5. You have 20 seconds to accept or reject a contact. If you miss a call, it will look similar to the following image. Choose **Clear contact** so you can accept another call.

---

**Transfer calls to a quick connect or external phone number**

You can transfer calls to people in a predefined list, called quick connects. You can also transfer calls to external phone numbers that you enter.

**To transfer to a quick connect or to an external number**

1. While you're connected to the contact, choose **Quick connects** on the CCP.
2. From the list of quick connects, choose the name of another agent to transfer the call to. (Your Amazon Connect administrator adds the names of agents to the list of quick connects.)

**Tip**

Agents see the quick connects of the queues in their routing profile, including the Default outbound queue.

Or, to call an external number, choose **Number pad**, enter the number you want to call, and then choose **Call**.
3. After the call is connected to the transfer destination, you can choose **Join** so the caller, the transfer destination, and you are in a conference call.
4. When the call is joined, the three of you can talk. Choose **Leave** to complete the transfer and exit the call.
5. Complete the after contact work and then choose **Clear contact**.
Manage transfer a call

After you initiate a transfer, the customer is placed on hold and you are connected to the transfer destination. The following image shows what actions you can take at this point.

- **Clear contact**: This button clears the active call.
- **Put all parties on hold**: Places you, the caller, and the transfer destination into a conference.
- **Disconnect the caller leg**: Disconnects the caller from the call.
- **Disconnect the transfer leg**: Disconnects the transfer destination from the call.
- **Mute your microphone**: Mutes the microphone for your side of the call.
- **Switch between talking to a call and the person to whom you’re transferring the call**: Allows you to switch between the call and the transfer destination.
- **Used to dial a number or enter digits into an IVR menu**: Enables dialing or entering digits for an IVR menu.

Transfer calls
Transfers create multiple contact records

A contact record is opened for a customer when they are connected to your contact center. The contact record is completed when the interaction with the flow or agent ends (that is, the agent has completed the ACW and cleared the contact). This means it's possible for a customer to have multiple contact records.

The following diagram shows when a contact record is created for a contact. It shows three contact records for a contact:

- The first record is created when the contact is connected to Agent 1.
- The second record is created when the contact is transferred to Agent 2.
- The third record is created when the contact is connected to Agent 3 during a callback.

Each time a contact is connected to an agent, a new contact record is created. The contact records for a contact are linked together through the contactId fields: initial, next, and previous.

For more information, see [About contact states](#).

Multi-party calls: Add additional participants to an ongoing call

You can add up to 4 additional participants to an ongoing customer service call, for a total of 6 participants.
By using quick connects or your number pad, you can add other agents, supervisors, or external participants.

For example, to help close a mortgage transaction, an agent at a financial services company can add a mortgage broker, the customer's spouse, a translator, and a supervisor to the call to help resolve any issues quickly.

For information about how multi-party calls differs from the default three-party calls, see Comparison: Three-party and multi-party calls.

**Important things to know**

- This feature is only available in CCPv2 and custom CCP using Amazon Connect Streams.js.

  - **IT administrators:**
    - Before enabling the multi-party calls feature, if you are using Contact Lens or planning to do so in the future, see Multi-party calls and Contact Lens. We do not support multi-party call architecture in Contact Lens and recommend you disable Contact Lens in the Set recording and analytics behavior block for such contacts.
    - By default, there can be three participants on a call (for example, two agents and a caller, or an agent, a caller, and an external party). Before enabling multi-party calling, see Comparison: Three-party and multi-party calls. To enable agents to connect up to six parties on a call, see Update telephony options.

  - **Developers:** In custom CCPs, use the updated Amazon Connect Streams API to enable multi-party calling, up to six parties. See the Amazon Connect Streams documentation on GitHub. Before enabling multi-party calling, see Comparison: Three-party and multi-party calls.

  - **AWS GovCloud (US-West):** You can't enable this feature using the console user interface. Instead, use the UpdateInstanceAttribute API or contact AWS Support.

**How to add participants to a multi-party call**

1. The following image shows the contact and you (the agent) on a call. The customer always appears at the top.
2. While you're connected to the contact, choose **Quick connects** to add another agent or the **Number pad** to make an external call. The caller is put on hold while you do this.

3. When you add the third participant to the call, you can greet and talk to them before adding them to the call (for example, tell them why you are adding them to the call).

The following image shows what the CCP looks like when you add a third participant to the call. The contact is on hold, and you're talking to the third party. Choose **Join** to take all parties off hold. Or, choose **Swap** to toggle between the parties on hold and the party you just called.
3. **Note**

Swap is only available when there are three parties on a call (for example, you, the caller, and another agent or external party). It is not available when there are more than three parties on the call.

4. When there are multiple agents on the call (for example, three agents and a caller), all agents on the call can view all parties and have the option to put any participant or another agent on hold, mute, and disconnect participants from the call.

5. Every time you add a new participant to the call, you are prompted to greet and talk to them before adding them to the call. Choose Join to take all parties off hold.
How to manage participants

Every agent on the call has access to the controls next to each participant’s number to mute, hold, or disconnect individual participants.

You can transfer a multi-party call to another agent, or disconnect yourself from the ongoing call.

Choose the More button to open the number pad and to create a task:
When do multi-party calls end?

A multi-party call stays up as long as the caller or the agent is on the call. For example, add an external party to a call and then you disconnect. The caller and external party continue the call.

If only third-parties are left on the line, the contact is terminated. However, as the agent you can choose to disconnect and allow only the caller and the third-party participants to remain on the call.

How to use the CCP to make outbound calls

Before you can make an outbound call, your contact center must be set up to allow agents to make calls. For more information, see Step 3: Set telephony in Create an Amazon Connect instance.

For information about the caller ID that's displayed when you make an outbound call, see Set up outbound caller ID.

### Note

**IT administrators**: For a list of countries available for outbound calls based on the Region of your instance, see Amazon Connect pricing. If a country is not available in your dropdown menu, open a ticket to add it to your allow list. For more information, see Countries you can call by default.
To make an outbound call

1. In your Contact Control Panel, choose **Number pad**.
2. Use the dropdown menu to choose the country, then enter the number.

3. Choose **Call**.

View a call transcript during ACW

At the end of a call, you can see an unredacted transcript of your conversation in the CCP or agent workspace. You can view the entire transcript for reference, and copy any useful text into your notes.

The call transcript displays any **categories** identified by Contact Lens. For example, in the following image, an issue has been identified at 22 seconds.
If a call is transferred to you from another agent, you will see an unredacted transcript of their conversation with the customer.

Customer sentiment score is not included in the CCP or agent workspace.

**Note**

**IT administrators**: This feature is available in the CCP and the agent workspace. To make this feature available to agents:

1. **Enable Contact Lens** for your Amazon Connect instance.
2. Add the following permissions to the agent's security profile:
   - **Analytics and Optimization** - **Contact Lens** - **Recorded Conversations** - unredacted (Access)
   - **Analytics and Optimization** - **Contact search** (View)
   - **Contact Control Panel (CCP)** - **Contact Lens data**

**How to use the CCP to manage chats**

The topics in this section explain how to use the Contact Control Panel (CCP) to manage chats.
Contents

- How to use the CCP to chat with contacts
- Search for quick responses in CCP
- Transfer chats to another queue
- How to use the CCP to make a call while on a chat

How to use the CCP to chat with contacts

When you set your status in the CCP to Available, Amazon Connect delivers calls or chats to you, based on the settings in your routing profile. An administrator can specify that up to 10 chat conversations can be routed to you at the same time.

You can't initiate chat conversations from the CCP.

Note

IT Administrators: To enable customers and agents to send attachments, such as files, through the chat interface, see Enable attachments to share files using chat and upload files to cases.

When a chat contact arrives, here's how you are notified:

1. If you enabled notifications in your browser, you'll get a pop-up notification at the bottom of your screen, like this:

   ![Incoming chat: John](image)

   Click here to open the contact control panel now.

   apps.com

2. If you're on the chat tab, the page displays the name of the contact and a button for you to connect to the chat.
3. If you're on the phone tab, a banner displays the name of the contact and a button for you to connect to the chat.

4. You have 20 seconds to accept or reject a contact. If you're on a chat, and another comes in but you don't accept it, a tab appears indicating the chat was missed.

5. Choose **Accept chat** to connect to the contact.

**Note**

Chat conversations must be accepted manually. There's no auto-accept for these conversations.
6. You'll see the full transcript of what the contact has already typed. If applicable, you'll also see what a bot or another agent has entered. In the following image, **John** is the name of the customer, **BOT** is the Amazon Lex bot, and **Jane** is the name of the agent.

![Chat Transcript](image)

**What do the timers at the top of the chat tabs mean?**

When you're in a chat conversation with a contact, you'll see two timers at the top of the chat tab. These timers tell you:

- How long the contact has been connected to your contact center. This includes the time spent with the bot, if you're using one.
• How long since the last text was sent. This can be either from the customer to the agent, or from
the agent to the customer. The timer is reset with texts message between the two. It is not reset
with each consecutive text message sent from a participant.

If you have multiple chat tabs open, an hour glass appears letting you know which ones are in an
After Contact Work (ACW) state. The timer indicates how long the contact has been in ACW.

What happens to missed chats?

Let's say you take a break but forget to change your status in the CCP from Available to Break.
Amazon Connect tries to route a chat to you for 20 seconds. Keep in mind that your admin can't
configure this amount of time.

After 20 seconds, the contact is counted as Agent non-response in the real-time metrics report and
the historical metrics report.
When you return from break and choose the chat tab, you'll see the missed contacts and how long they've been there. Each contact occupies a slot. With all of your slots are occupied, Amazon Connect won't route any more contacts to you. You must clear the missed contact so more contacts can be routed to you.

⚠️ **Important**

If you're set up to handle contacts while already on another channel (for example, voice, chat, and task), you still must clear the missed contact before any other contacts on any other channel can be routed to you.

You can clear the slots so that chats are routed to you again. For each missed contact, choose the banner, and then choose **Clear contact**.

**How to format messages**

When composing a chat message, you have the ability to format your message. This enables you to add structure and clarity to your support messages. You can add the following formatting:

- **Bold**
- **Italic**
- **Bulleted list**
To get started, highlight the text you want to format, and then select a the formatting options from the toolbar at the bottom of the chat window. You can see exactly what the message looks like before sending it.

⚠️ Tip
Developers: Enable this feature from the chat user interface. For instructions, see [Enable text formatting for your customer's chat experience](#).

### Search for quick responses in CCP

Use either of the following methods to search for quick responses:
• Choose the star icon in the rich text toolbar.

• Enter /# in the box used to compose messages.

**Note**

- The star icon only appears when contact is initiated.
- To see the star icon in CCP, you must have at least 1 activated quick response associated with the current agent routing profile.

The following image shows a quick response found by entering a shortcut (/#G1) in the agent application.
Transfer chats to another queue

When a chat is transferred from a bot to an agent, or from an agent to another queue, all context is preserved. This context lets the next agent read all previous messages in that contact.

To transfer a customer to another queue

1. Choose the Quick Connect button at the bottom of the CCP page.
2. Choose or search for the queue you want to transfer to, and then choose the transfer button.

3. You'll see a confirmation message: Chat transferred. You're now doing After Contact Work (ACW) for the customer. Choose **Close** to end the contact.
How to use the CCP to make a call while on a chat

Let's say you're chatting with a contact and you want to consult with someone else. While you're on a chat, you can use the updated CCP to make outbound calls using the number pad and phone number quick connects.

Note the following limitation:

- You can't access agent quick connects while you're on a chat.
- Agents can receive calls while on a chat only if they are assigned to a routing profile that allows cross-channel concurrency.

To make an external call while you're on a chat

1. In the CCP, choose the phone tab.
2. Choose **Number pad**.
3. Enter the external number you want to call, and then choose Call.
4. You'll be connected to the call at the same time the chat is still ongoing, as shown in the following image.
5. To go to the chat conversation while you're on the phone, choose the chat tab.

6. To end the phone conversation, choose the phone tab, choose **End call**, and then choose **Clear contact**. You're still connected to the chat conversation.

**Can't make outbound call to another agent**

If you're on a chat and having trouble making an outbound call to another agent, it could be because that agent's routing profile is not set up to allow them to take calls while on a chat or task contact. They need to be assigned to a routing profile that allows **cross-channel concurrency**.

**Can't see phone number quick connects in the CCP**

**Agent quick connects** are not visible in the CCP while you're on a chat.

If you can't see **phone number quick connects** in your CCP, however, check that the phone number quick connect has been added to your queue as described in **Step 2: Enable agents to see quick connects**.
Enable agent quick connects for calls during a chat

To enable agents to consult over the phone with each other while they are on chats, your Amazon Connect administrator needs to set up a direct dial number (DID) that routes to the agent. This configuration incurs additional costs.

How to use the CCP to work with tasks

The topics in this section explain how to use the Amazon Connect Contact Control Panel to manage tasks.

Contents

• Accept a task
• Create a new task
• Transfer a task

Accept a task

1. Whenever you set your status in the CCP to Available, Amazon Connect can deliver tasks to you, based on the settings in your routing profile.
2. When a task arrives, choose **Accept task**. You have up to 30 seconds to accept a task (10 seconds more than accepting a call or chat).

3. Review the description of the task, and choose the links as needed to complete the task.
4. When you've completed the task, choose **End task**.

5. You will then be in ACW. When finished, choose **Close contact**.
Create a new task

You can create a task any time, even when your status is Offline. And you can assign a task to anyone who has a quick connect, including yourself.

You can create a task, which starts the task immediately. Or you can schedule the task to start on a future date and time.

1. Open the CCP. Select the **Task** tab, and then choose **Create task**.
2. Complete the **Create task** page. When you choose **Assign to**, you can assign a task only to someone or a queue that has quick connect.

Choose **Create**.

CCP only

The following image shows the option to create a task in the CCP.
3. If you chose yourself, the task is routed to you. Choose **Accept task**.
Create a scheduled task

You can schedule a task to start on a future date and time.

1. Complete the steps to create a task. For example, add a **Task name** and **Assign to** a quick connect.

2. In the **Scheduled date / time** section, choose a future date and time, and specify the timezone. You can schedule a task up to six days in future.

3. If you want to clear all values in the **Scheduled date / time** section and start over, choose **Clear scheduled date / time**.

Transfer a task

You can transfer a task that's assigned to you to another agent or queue.

1. Open the task you want to transfer, and then choose the quick connect icon.
2. Choose from the list of people or destinations listed under **Quick connects**, and then choose the transfer icon.
Use Customer Profiles in the agent workspace

To help agents deliver more efficient and personalized customer service, Amazon Connect enables you to combine information from external applications, such as Salesforce, Zendesk, ServiceNow, or other Customer relationship management (CRM) products, with contact history from Amazon Connect. This creates a customer profile that has all the information agents need during customer interactions in a single place.

With a single view of customer information including their product, case, and contact history, agents can quickly confirm the customer's identity and determine the reason for the call or chat.
Currently, Amazon Connect Customer Profiles can be used in compliance with GDPR and is pending additional certifications held by Amazon Connect.

The following image shows the agent workspace; for the purposes of this documentation, an Amazon Connect Customer Profiles image is featured. The agent workspace is designed for efficient multi-tasking, enabling simultaneous handling of calls, chats, and tasks, while providing quick access to customer profile information all within the same browser window.

1. **Cases**: Status, reference Id, title, source, updated date, and more information related to cases ingested from 3P application such as Zendesk and ServiceNow, in addition to cases created and managed using Amazon Connect Cases.

2. **More information**: Additional information contained in the customer defined Attributes field of the profile, as well as further profile information such as cell phone number and shipping address. This information will be sorted alphabetically to help an agent quickly locate the information they need.

3. **Contact history**: Date, times, and duration when this customer contacted your contact center in the past.

4. **Product purchase history**: All the assets purchased by a customer can be populated here. The data is ingested from an external app such as Salesforce or Zendesk that you've integrated with Customer Profiles.
Accept incoming contacts with Customer Profiles

When a call or chat is connected to your Contact Control Panel (CCP), Amazon Connect Customer Profiles, in the same browser window, automatically populates the customer profile that may match the incoming phone number for a voice interaction and Name for a chat interaction.

Tip

You can change autopopulation behavior if you wish. For more information, see Use contact attributes to autopopulate customer profiles.

Before agents can access customer profiles, the Amazon Connect administrator must enable the Customer Profiles feature, grant agents the appropriate permissions, and integrate Customer Profiles into your agent workspace. For more information, see Enable Customer Profiles for your instance.

Example 1: Auto-populate the customer profile

As soon as Amazon Connect Customer Profiles matches the phone number (voice) or customer name (chat) with an existing customer profile, it automatically displays the profile even though you may not have accepted the contact yet.
The following image shows what your Contact Control Panel (CCP) may look like when there's an incoming chat. A customer profile has been found that matches the customer, and Amazon Connect is loading the data.

This next example shows what it might look like after you've accepted and joined the chat, and Amazon Connect displays the customer's profile. In this case, Amazon Connect found the customer's profile based on their email address. If this were a voice call, by default Amazon Connect would match the customer's profile based on their phone number. Your IT department can customize this behavior to search for the profile based on other information about the contact.
• Choose **Associate** to associate the contact record of the current contact with the customer profile, and then choose **Confirm**.
• If you choose **Associate** by mistake, you can continue to browse other customer profiles, and associate the contact with a different customer profile. Or, if you have been assigned **Create permission**, you can create a new profile.

You can associate a contact with customer profile multiple times during an interaction, including during After Contact Work (ACW) time. Only the most recent association remains, before you clear the contact.

**Example 2: Accept incoming contact, no customer profile found**

If no results are returned when a call or chat comes in, do the following:
1. Search for the customer's profile using any search key available in the search drop down menu. For example: phone, name, email, account id, or any custom search terms you specify. For example, if you have **Social security number** (SSN) defined as one of your identifiers, SSN will automatically be available as a search term for agents to use in the Agent Workspace.

2. If no customer profile is found, create a new profile for the contact. The only required information is first name.
In the following image, the agent searched for **John Doe**. No matches were found so they chose **Create profile**.

**Example 3: Search when not on contact**

When there are no incoming contacts, you can search for customer profiles using any search key available in search drop down menu. For example, phone, name, email, or account id. For example, you might want to use this time to search for previous contacts, or completing a profile.
Example 4: Autopopulate results in multiple profiles found

In some cases, multiple profiles may be returned for the same call or chat. Use the profile information to verify the customer's identity. For example, ask the customer to verify their email address or account number, and then associate the contact with the right customer profile. Agents can also ask customers for additional information they can use in search and identify the right profile in order to associate it to the interaction.
Accept incoming contacts with Customer Profiles
Create a new customer profile in the agent workspace

Let's say you're on a chat and there's no customer profile for the contact. You can create a new customer profile for them.

1. Choose **Create profile**.
2. Choose **This is the current connected customer**. This tells Amazon Connect to link the customer profile to the contact ID for the current customer.

   If you don't select this check box, the profile isn't associated with the current contact. This is useful when a contact is calling from someone else's number.

   Enter information in the required boxes, and then choose **Save**.

   **Tip**

   Agents can use any of these customer Identifiers in the Agent Workspace to find the profile that belongs to the customer on the interaction.
3. You'll receive a verification page that the contact has been created.
4. You can continue the conversation with the customer.

**Search for a customer profile in the agent workspace**

Even when you're not on a contact you can search customer profiles. This is helpful in cases where, for example, you want to return to a customer profile.

1. In the **Search** box, select the key you wish to use to search for a profile and enter the value you wish to search with. For example, you can select *phone* from the drop down menu and enter `206-555-2322` in the input field to search.
2. If more than one result is returned, you can review the profile information to identify the contact that you want.
Tip

- You can enter a search term without having to select an attribute for phone number, name, email, Account ID, or profile ID. The agent workspace will automatically detect the values type and run a search for matching profiles.
- Searching for Profiles in the agent workspace will return profiles that match your exact search value.

Use Cases

A case represents a customer's issue. A case is created to record the customer's issue, the steps and interactions taken to resolve the customer's issue, and the outcome.

If you have permission to view cases then you will see the Cases tab in the Amazon Connect agent workspace. The following image shows an example Cases tab in the agent workspace.
Contents

- Search and view cases
- Add comments to a case
- Create a case
- Associate a contact with a case
- Edit a case
- Create a task from a case

Search and view cases

You can search cases using a keyword match. Amazon Connect searches data across all system and custom fields. The results are sorted from most-recently to least-recently updated case.

If you are on a contact, and the contact has been associated to a customer profile, then search automatically filters to cases of current customer.
Regardless of whether you are on a contact, you have the option to do a general search. If you are on a contact and want to search beyond the current customer, clear the selection for **Cases of current customer only**.

**View a case**

When you select any of the cases in the search results to view the case, a new tab opens. This enables you to have multiple cases open at the same time.

If you add a **Cases** block to a flow, and configure it with **Link contact to case** enabled, then cases will open automatically when the agent accepts the contact.

**Activity feed**

The activity feed shows calls, chats, tasks, and comments from the most recent to least recent Started data.

Contacts will have an indicator of Ongoing or Completed. If the contact was completed, there will a Completed/Terminated date/time and a link to **Contact details** that takes user directly to the **Contact details** page.

Only users who have access to this page will be able to see contact details for a given contact. Even within this page, there are more granular permissions so different users may see different information. Information might include: basic contact details/contact attachments, transcripts and recordings with Contact Lens categories, sentiment, and summaries, recordings, etc.
More information

There may be additional information for agents to view and populate on the More information tab, depending on the case template is designed.

Add comments to a case

Agents have the ability to view and add comments to a case.

You cannot add a comment to a case in Closed status. You can re-open the case and then leave the comment.
Create a case

To create a case, you must be on a contact (call, chat, or task) and have associated the contact with a customer profile, as shown in the following image.

For a case to be created:

- The **Status** must be **Open**.
• All required fields must be filled in.

Customer name

Each case that is created is connected to a customer profile from your Amazon Connect instance. While viewing the case details page, an agent can click or tap the customer’s name to open the associated Customer Profile in a different tab. Or, the agent can choose More (...) to copy the customer name or profile ID to the clipboard. On new case templates, the customer name appears by default on the case details page. You can rearrange this field on your case template, or even remove it entirely.
Associate a contact with a case

You can associate the contact to an existing case, such that the contact will appear on the activity feed of the case with indicator **Ongoing**.

Edit a case

To edit a case, the agent chooses **Edit** and **Save** to save any changes.

You can edit a case only when it is not in a **Closed** status. If the case is **Closed**, you must update the status, then choose **Edit** to make your changes.
Create a task from a case

In the agent workspace, you can add a task from a case. In the Contact Control Panel (CCP), you will see the task creation form.

When you create a task from a case, the task is automatically associated with the case and it appears on the activity feed.
Use Amazon Q in Connect in the agent workspace

Note

**Powered by Amazon Bedrock:** AWS implements [automated abuse detection](#). Because Amazon Q in Connect is built on Amazon Bedrock, users can take full advantage of the controls implemented in Amazon Bedrock to enforce safety, security, and the responsible use of artificial intelligence (AI).

Amazon Q in Connect is a generative AI customer service assistant. It is an LLM-enhanced evolution of Amazon Connect Wisdom that delivers real-time recommendations to help contact center agents resolve customer issues quickly and accurately.

Amazon Q in Connect automatically detects customer intent during calls and chats using conversational analytics and natural language understanding (NLU). It then provides agents with immediate, real-time generative responses and suggested actions. It also provides links to relevant documents and articles.

In addition to receiving automatic recommendations, agents can also query Amazon Q directly using natural language or keywords to answer customer requests. Amazon Q works right within the Amazon Connect agent workspace.
The following image shows how recommendations may appear in the agent workspace when an agent is on a call or chat.

1. The agent is on a call.
2. The agent can ask natural-language questions.
3. Amazon Q in Connect provides a response that the agent can share directly with the customer. For example, they can copy and paste the response into a chat, or read it over the call.
4. Amazon Q in Connect provides more information for the agent, for example, a summary of the solution or of the next steps they should take.
5. Amazon Q in Connect provides links to specific articles.

Contents
- Search for content using Amazon Q in Connect
- Use real-time recommendations from Amazon Q in Connect

Search for content using Amazon Q in Connect

With Amazon Q in Connect agents can use natural language to search across connected knowledge sources to receive generated recommendations, like actions to take and links to more information.
For example, you can type questions or phrases in the search box (such as, "how long after purchase can handbags be exchanged?") without having to guess which keywords will work. Amazon Q in Connect searches the connected sources, and returns a specific solution generated from your knowledge content along with links to relevant information.

You can search for content at any time: while on a contact, on After Contact Work, or between contacts.

**To search for content**

1. In the search box, type words or phrases in natural language.

   The following image shows an example of a natural language query and the solution that is displayed.
2. If more information is needed, choose the article that you want to view.
3. The article appears in a new tab. For example, the following image shows the Cancellation policy article.
4. The list of search results is cleared only after you complete ACW and choose **Clear contact**, or select the **Close** icon next to the search box.

### Use real-time recommendations from Amazon Q in Connect

This topic explains how agents who are using Amazon Q in Connect in the agent workspace can interact with real-time recommendations that are generated for chats. If Contact Lens is enabled, the recommendations appear for calls as well.

The recommendations point you to information related to the current conversation with the customer.

The following image shows how an article may appear in the agent workspace when you're on a call.
1. The agent is on a call.

2. The agent can ask natural-language questions.

3. Amazon Q in Connect provides a response that the agent can share directly with the customer. For example, they can copy and paste the response into a chat, or read it over the call.

4. Amazon Q in Connect provides more information for the agent, for example, a summary of the solution or of the next steps they should take.

5. Amazon Q in Connect provides links to specific articles.

**Use Voice ID**

This topic shows how Voice ID features appear in your Contact Control Panel (CCP).
1. You receive an incoming call.

2. The caller is not yet enrolled in Voice ID so you choose **Enroll**.

3. A message is displayed that Voice ID is sampling the caller's voice. It requires 30 seconds of speech (excluding silence).

4. The caller is now enrolled in Voice ID. This example also shows the caller's **Fraud risk** as lower than the threshold.

**Verification of an enrolled caller**

After a customer is enrolled in Voice ID, when they call your contact center again, you can verify they are who they say they are.
1. You receive an incoming call.

2. The caller is already enrolled in Voice ID, and their status is **Authenticated**. You can choose to re-evaluate authentication using Voice ID.

3. A message is displayed that Voice ID is evaluating the caller's speech. It requires between 5-10 seconds of speech, not including silences.

4. The caller has been authenticated by Voice ID. This example also shows the caller's **Fraud risk** is lower than the threshold.

**Caller has opted out**

The following image shows what appears in your CCP when a caller has opted out of Voice ID.

1. You receive an incoming call.
2. The caller has previously opted out of Voice ID.
3. You have the option to enroll them.

**Authentication status = Not authenticated**

When an enrolled caller calls your contact center, Voice ID may return a result of **Not authenticated**. This means Voice ID was unable to authenticate a caller's speech. The authentication score for the caller is lower than the configured threshold.
The previous images show that the Fraud risk can be High or Low, independent of whether the caller is authenticated.

**Authentication status: Inconclusive**

When an enrolled customer calls your contact center, Voice ID may return a result of Inconclusive: Voice ID was unable to analyze a caller's speech for authentication. This is usually because Voice ID did not get the required 10 seconds to provide a result for verification.
Troubleshooting Issues with the Contact Control Panel (CCP)

Troubleshooting Contact Control Panel (CCP) issues requires support from your network operations, system administrator, and virtual desktop (VDI) solution teams to collect the appropriate level of information to identify root cause and drive resolution. To help determine the appropriate resources to engage, it's important to break issues down into those with similar symptoms. The following guidance has been helpful in assisting Amazon Connect customers in resolving CCP issues with their operations support teams.

Contents

- Use the Endpoint Test Utility
- Common Contact Control Panel (CCP) Issues
- Download CCP logs
- Troubleshooting Tools and Information
- Mobile phones (iPhone, Android) and iPads are not supported
- Problem using the CCP: Agents can't make an outbound call
- Internal firewall prevents access to chat or case attachments
- Humming sound in headset: Verify the headset and browser sample rates
- One-way audio from customers?

Use the Endpoint Test Utility

To validate connectivity to Amazon Connect, or when your agents are experiencing problems with the Contact Control Panel (CCP), we recommend using the Amazon Connect Endpoint Test Utility.

The Amazon Connect Endpoint Test Utility performs the following checks:

- Validates that the browser being used supports WebRTC.
- Determines if the browser has appropriate access to media devices (microphone, speakers, etc).
- Performs latency tests for all active Amazon Connect Regions.
- Performs latency tests to a specific Amazon Connect instance, if provided.
- Validates network connectivity across required ports for media streams.
The complete results are available for download as a JSON file. You can copy the results to include in a support ticket. You can also load the results file into the tool by selecting the Load previous results option. This option displays the contents of the file visually and makes it easier to analyze the results. Additionally, you can download a bookmark specifically for the provided instance to make future tests easier to run.

**Parameters to customize the Endpoint Test Utility**

You can use the Endpoint Test Utility as is without any customizations. However, if you want to customize it, use the following URL parameters:

- **lng**: Change the language of the tool. Currently supported languages are English, Spanish, and French. It accepts the following values:
  - en (default)
  - es
  - fr
- **autoRun**: Run the tool automatically. It accepts the following values:
  - true
  - false (default)
- **connectInstanceUrl**: Not used by default. You can specify the Amazon Connect instance in the URL. It must start with https.
- **regions**: A comma-separated list of region codes for the AWS Regions that you want to test. For example regions=us-east-1,us-west-2.

Example customized URL:


**Common Contact Control Panel (CCP) Issues**

The following are common issues encountered when using the Amazon Connect CCP.

- **CCP does not initialize/connect**—The most common causes are missing port/IP allowlist entries, not allowing browser microphone access, or not answering your external device. Be sure that you
have added to the allowlist all IPs covered in the Set up your network section of this guide, and that you have allowed microphone access to your browser when prompted.

- **Periodic connection errors**—The most common cause is network contention, or there may have been an ipranges.json update and the new entries have not been added to the allowlist. For more information, see the Set up your network section of this guide.

- **Missed calls, state change delays, and CCP unresponsive**—In most cases, this is intermittent and directly correlated with resource contention in the agent's workstation, network, or both. This can be made worse, or caused directly, by a poor, unstable, or strained connection to AWS resources at the private WAN/LAN, public WAN levels, or local workstation resource contention.

The following are common issues with call quality when using the CCP. Call quality encompasses a large range of potential causes and is best approached by first identifying the types of issues that you're having.

- **Latency/cross-talk**—in a voice connection manifests as a delay between when something is said and when the person on the other end hears it. In some use cases that require a lot of conversation, high latency can create situations in which both parties are talking over each other. The PSTN (public switched telephone network) and agent latency need to be calculated in this scenario to identify contributing factors and take action to reduce PSTN latency, agent latency, or both. For more information, see the PSTN and agent connection latency section of this documentation.

- **One way audio**—is when the agent can't hear the caller or the caller can't hear them. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. It and can also be related to browser microphone permissions or headset issues. For more information, see the How to determine whether a workstation is the source of problems section of this guide.

- **Volume increase or decrease**—can happen at the beginning or intermittently during the call, and it's important to differentiate the two for troubleshooting purposes. Typically, this relates to forwarding calls to or from Amazon Connect that inherit this from an issue with the third party transfer.

- **Audio choppy, cutting out, echo, reverb, or other signal noise**—could also manifest as a robotic sound or other distortion making it difficult for either the agent, caller, or both parties to understand what's being said. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. For more information, see the How to determine whether a workstation is the source of problems section of this guide.
• **Wobble**—is the effect that media codecs can have on audio that manifests as the slowing down and speeding up of audio to combat high jitter and latency. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. For more information, see the [How to determine whether a workstation is the source of problems](#) section of this guide.

• **Disconnects**—can happen at any point in the call. It is important to note when during the call that the disconnections occur to identify a pattern. For example, disconnects on call transfers to a specific external number typically relate to forwarding calls to or from Amazon Connect that inherit this from an issue with the third party transfer. They can also be related to circular transfers, which means transferring calls out of Amazon Connect and back in the same call.

**Download CCP logs**

The Contact Control Panel logs store agent actions and timing.

**To download CCP logs**

1. On the agent's desktop, in their CCP, choose **Settings, Download logs**.
2. The `agent-log.txt` file is saved to your browser's default directory. After the file is downloaded, you can change the name of the file the same way you rename any other file on your computer. You can't customize the file name before the file is downloaded.

### Troubleshooting Tools and Information

The following tools and information can be helpful with troubleshooting issues with Amazon Connect.

- **Instance ARN**—Provide your instance ARN (Amazon Resource Name) when you contact AWS support so that they can see the activity in your Amazon Connect instance. You can find the ARN for your instance on the Overview page that you access by choosing the alias of the instance from the Amazon Connect console.

- **Call recordings**—are very useful, not only to illustrate and determine reported behavior, but also to rule out audio issues from the agent's side. Recordings in Amazon Connect are done at the instance side of the interaction, before the audio traverses the agent connection. This allows you
to determine if the audio issue was isolated to the agent's side of the interaction or if it existed in the audio received by the agent. You can find call recordings associated with a contact in the Contact Search report.

- **Contact IDs from the contact record** — Provide when you contact AWS support.
- **Agent desktop performance/process logs** — Can help rule out local resource/network contention.
- **Contact Control Panel (CCP) logs** — To track agent actions and timing. To download CCP logs, choose the settings cogwheel in the CCP, and then choose **Download logs**. The logs are saved to your browser's default download directory.
- **Network utilization logging/monitoring** — Specifically for latency and dropped packets on the same network segment as your agents.
- **Private WAN/LAN network diagram** — Outlining connection paths to the edge router to AWS to explain network traversal.
- **Firewall allowlist access** — To verify that IP/port ranges are added to the allowlist as described in **Set up your network**.
- **Audio capturing and analytic tools** — For latency calculations from the agent's workstation.
- **AWS region latency test tools** — Use the **Endpoint Test Utility tool**.

## Gathering Helpful Information using the Streams API

For tracking and troubleshooting issues at scale, collecting data surrounding overall call quality is recommended. Anytime poor call quality is experienced, agents can note the current time and corresponding disposition code by using the disposition key chart, as shown in the following chart. Alternatively, you can use the Streams API to incorporate your own report and issue feature in the custom CCP to write these dispositions with corresponding call information to a database, like Amazon DynamoDB. For more information about the Amazon Connect Streams API, see the GitHub repository at [https://github.com/aws/amazon-connect-streams](https://github.com/aws/amazon-connect-streams).

### Example Agent Issue Report Disposition

The following example disposition keys are listed by symptom, scenario, and severity.

#### Symptom

- **S** — Softphone error
- **M** — Missed calls
- **L**—Latency causes poor quality
- **P**—Starts off OK, gets progressively worse over time
- **D**—Disconnected calls
- **W**—One way audio; for example, the agent can hear the customer, but the customer cannot hear the agent
- **V**—Volume too quiet or too loud
- **C**—Choppy/cuts in and out intermittently

**Scenario**

- **O**—Outbound call
- **I**—Inbound call
- **T**—Three-way call

**Severity**

- **1**—Small impact, but can use the CCP effectively
- **2**—Medium impact, communication is difficult, but can still service calls
- **3**—Large impact, cannot use the CCP to take calls

**Examples**

- 5:45PM agentName LT2 (latency on a three-way call with medium impact).
- 6:05PM agentName DO3 (disconnected outbound call with large impact).
- 6:34PM agentName MI3 (missed inbound call with large impact).

**Analyzing the Data**

The following guidelines can assist you in analyzing the data to identify issues in your environment.

- Use the Contact record / Contact search report to identify the contact IDs for the contacts during which call quality issues occurred. The contact record includes a link to the associated call recording, and additional details that you can use for symptom verification and to provide to your AWS support representative.
• Use the agent name and timestamp in the contact record to get a sense of the types of issues you're experiencing and their prevalence by agent, symptom, scenario, and severity over time. This will allow you to see if issues are happening around the same time, surround a specific event, or are isolated to specific agents or agent actions. You can also easily identify and access associated call recordings and associated contact IDs available if you need to engage support.

• Correlate data sources, such as local network logs, CPU/disk/memory utilization and process monitor logs from the operating system on the client workstation. This lets you correlate events by agent over time to rule out local resource contention as a cause or contributor.

• Analyze data by symptom and scenario reported per minute or per hour to create heat maps of an issue by type and severity by agent over time. Doing this is especially helpful in environmental troubleshooting as you may find clustered impacts associated with scheduled activity like backups or large file transfers.

• If you can't find any evidence of local resource contention or derive any noteworthy correlations, you can use the contact IDs collected to open a support case. If issues experienced are intermittent in nature, they most likely relate to issues with the agent's workstation, network connectivity, or both.

Validation Testing

Voice quality issues can have many contributing sources. It's important to run controlled tests and monitor the same environment or workstation as those reporting the issue, and be able to reproduce the same use cases. Consider the following general testing recommendations for measuring and gathering data to investigate voice quality issues.

PSTN and Agent Connection Latency

For troubleshooting cross-talk issues, you need to differentiate and measure agent and raw PSTN latency contributions, as they require different remediation efforts.

• \([\text{overall\_latency}]\) is the total latency experienced between caller and agent. This latency can be calculated as \([\text{overall\_latency}] = [\text{agent\_latency}] + [\text{pstin\_latency}]\).

• \([\text{pstin\_latency}]\) is the latency between Amazon Connect endpoint and the caller. This latency can be calculated as \([\text{pstin\_latency}] = [\text{overall\_latency}] - [\text{agent\_connection\_latency}]\). This latency can be improved by using a different Amazon Connect Region location or avoiding external and circular transfers to geographically distant endpoint locations.
[agent_latency] is the latency between Amazon Connect endpoint and the agent. This latency can be calculated as \[\text{agent_latency} = \text{overall_latency} - \text{recording_latency}\]. This latency can be improved by using AWS Direct Connect for agents on-premises, avoiding the use of VPN connections, improving private WAN/LAN performance/durability, or using an Amazon Connect Region location closer to your agents. Depending on your use case, selecting a different Region selection may also increase [pstin_latency].

Amazon Connect leverages CloudFront for connectivity. Not all CloudFront ranges are advertised over AWS Direct Connect. This means not all URLs generated by Amazon Connect are reachable over a Public Virtual Interface.

[redirect_latency] is the latency resulting in redirecting audio to an external device. This latency can be calculated by measuring [overall_latency] once with redirect and once without and take the difference between the two.

[forward_latency] is the latency resulting in forward calls to or from Amazon Connect. This latency can be calculated by measuring [overall_latency], once with forward and once without, and take the difference between the two.

**Measuring Latency**

In addition to the steps below, see [Measure latency for validation testing and troubleshooting in Amazon Connect](#).

- Reproduce your use case. Any deviations need to be measured and accounted for, because they skew test results.
- Match production controls and environment as much as possible. Use the same flows, phone numbers, and endpoint locations.
- Note the geographical locations of your callers, agents, and external transfer destinations, where applicable. If you are servicing multiple countries, each country should be tested individually to provide the same test coverage that your agents experience in production.
- Note mobile and land line use in your tests. Mobile networks can add latency and need to be measured and considered for customer, agent, and transfer endpoints, where applicable.
- Reproduce the business use case. If the agents use conference and transfer, be sure to test those scenarios. If circular transfers occur, which are not recommended, be sure to test those as well.
- Reproduce the agent environment by including the workstation environment, located on the same network segment, and using equipment your agents would use.
Requirements for Testing Latency

To perform effective testing for latency, the following are required:

- Call recording enabled to capture [agent_latency]. Without call recording, you can calculate only [overall_latency].
- A customer phone source. For testing, confirm call quality on an actual call from a customer.
- An agent phone, if redirecting audio to an external device. You must be able to record the input and output of this device.
- A third-party transfer endpoint, if applicable. Testing is best when performed on actual calls or transfers from a third party.
- An agent workstation with sound recording or analysis software.
- Reproducible use cases. Troubleshooting can be difficult for issues that cannot be reproduced.
- NTP or other method to sync timestamps to facilitate identifying specific contacts and when they occurred, especially when activity is occurring across multiple time zones.

Testing Inbound Calls Using a Soft Phone

This process allows you to complete a latency test scenario in about 15 seconds. Analyzing the results and marking timestamps takes approximately 1-2 minutes per recording.

1. Go to a quiet location.
2. Configure agent workstation to play audio from external speakers and make sure they are turned up.
3. Use the agent workstation to log in to the CCP.
4. Start recording using an audio capturing tool on the agent workstation.
5. From the customer's phone source, use a speaker phone to call the incoming number for your Amazon Connect instance. This could really just be any external phone source to simulate a customer call.
6. Answer the incoming call using the soft phone on the agent workstation.
7. Make sure that the customer phone is not muted.
8. On the customer side, use an object or your hand, tap loudly on the desk or table, and then immediately mute the customer phone.
9. Wait 3 or more seconds. Repeat steps 7-8 at least 3 times.
10. Stop recording on the agent workstation.

11. Open the recording in your audio analysis tool. You should be able to see both the initial tapping sound that you made on the desk, and the tapping sound on the agent line on the other end. Take the three deltas and average for your [overall_latency].

12. Optionally, to calculate [agent_latency], open the associated Amazon Connect call recording in your audio analysis tool. You should be able to see both the initial tapping sound and the sound when it arrives to the agent at the other end. Take the three deltas and average for your [recording_latency]. [agent_latency] = [overall_latency] - [recording_latency]. Repeat as needed.

Modify the test plan as necessary to fit your use case. As the steps change, the process of recording and analyzing the audio is the same. If you need to test conferences and transfers, take measurements as normal, and then take another measurement when the conference is active with the third party transfer endpoint.

Interpreting the Test Results

The impact of increasing [overall_latency] begins to be noticeable at approximately 300ms and can result in crosstalk above 500ms. The impact, and what level of latency is considered acceptable, depends on your use case. For recommended remediation efforts for decreasing latency, see the PSTN and Agent Connection Latency.

Mobile phones (iPhone, Android) and iPads are not supported

The default version of the Contact Control Panel (CCP) does not work with mobile devices such as iPhones and iPads.

You can set up your CCP to forward the audio portion of the call to your mobile device. For instructions, see Forward calls to a mobile device (iPhone, Android).

Problem using the CCP: Agents can't make an outbound call

The top reason most agents can't make outbound calls from the CCP is because their instance of Amazon Connect has not been set up to make outbound calls.

To enable agents to make outbound calls

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL. The following image shows the Amazon Connect virtual contact center instances page, with a box around the instance alias.

3. In the navigation pane, choose **Telephony**.
4. To enable outbound calling from your contact center, choose **I want to make outbound calls with Amazon Connect**.
5. Choose **Save**.

**Internal firewall prevents access to chat or case attachments**

This topic is for developers who need to investigate issues that may occur when using attachments with the chat channel in Amazon Connect, or when using attachments to upload files to cases.

The following issues may cause attachments to not display for your agents using Amazon Connect chat or Amazon Connect Cases.

**Internal firewall settings are preventing access**

Check that your firewall isn't preventing agents from accessing the files in your Amazon S3 bucket. You may need to add the Amazon S3 bucket where your files are stored to your domain allowlist. For more information, see [Set up your network](#).

**Attachments are too large, too many, or don't meet file type requirements**

Check that the attachments meet the size, number, and file type requirements. For more information, see [Amazon Connect feature specifications](#).
To calculate the size of an attachment (artifactSizeInBytes), use a third-party tool such as `File.size`.

Humming sound in headset: Verify the headset and browser sample rates

If the agent's audio device does not support up to 48khz and the browser asserts a sample rate of 48khz, audio issues such as an audible humming sound may be present in the agent's outgoing audio. This has been seen with Firefox but not with Chrome.

Perform the following steps to verify your headset and browser sample rates.

**Verify Firefox sample rate**

1. Open the agent's CCP in FireFox, and set their status to **Available**.
2. Accept a call.
3. Open a second Firefox tab, and type `about:support` in the Search box.
4. Scroll down the page to **Media**.
5. Verify that the sample rates for the input and output devices are **48000**, as shown in the following image.

![Firefox sample rate](image)

**Verify Chrome sample rate**

1. Open the agent's CCP in Chrome, and set their status to **Available**.
2. Accept a call.

3. Open a second Chrome tab, and type `chrome://about` in the Search box.

4. Scroll down the page and choose `chrome://media-internals`.

5. On the **Audio** tab, choose the **Input Controllers** and verify that the sample rate is **48000**. Then verify the sample rate for the **Output Controllers**.
Verify Chrome sample rate

```
Verify Chrome sample rate
```
One-way audio from customers?

If an agent can hear the customer, but the customer can't hear the agent, this may be the result of an application taking exclusive control of agent's mic/speaker.

You can search the internet for articles that explain how to turn off exclusive-mode for a Windows audio playback device. For example, Turning off Exclusive Mode in Windows 10 Home Edition or How do I turn off Exclusive-Mode for a Windows audio playback device?.

To fix sound problems on a Mac, see Change the sound input settings on Mac.
Release notes for Amazon Connect

We recommend subscribing to the RSS feed so updates to these notes are delivered to your Inbox. Click the **RSS** link (under the topic title **Release notes**) to subscribe.

**December 2023 Updates**

**Contacts Answered/Abandoned in X**

On the **Real-time metrics** page, you can define custom thresholds for **Contacts Abandoned in X** and **Contacts Answered in X**, where X is a time range that you specify.

**November 2023 Updates**

**Customer Profiles provides a generative AI powered customer data mapping capability**

Customer Profiles provides a generative AI powered customer data mapping capability that significantly reduces the time needed to create unified profiles, which allows you to create more personalized customer experiences more efficiently. For more information, see the [Generative AI powered data mapping](#).

**No-code UI builder for step-by-step guides**

This feature allows you to create and manage the UI pages shown to agents in step-by-step guides. Using a drag-and-drop interface you are able to define static and dynamic content for the agent’s UI. This includes layouts, styles, and dynamic data, which enables you to control the look and feel of your agent’s experience. With this capability, you are able define what gets displayed in your agent's UI during the step-by-step guided experience. For more information, see the [No-code UI builder](#) documentation.

**Added Amazon Q in Connect**

Amazon Q in Connect is a generative AI customer service assistant. It is an LLM-enhanced evolution of Amazon Connect Wisdom that delivers real-time recommendations to help contact center agents resolve customer issues quickly and accurately.
Amazon Connect automatically detects customer intent during calls and chats using conversational analytics and natural language understanding (NLU). It then provides agents with immediate, real-time generative responses and suggested actions. It also provides links to relevant documents and articles.

For more information, see Use Amazon Q in Connect for generative AI–powered agent assistance in real-time and the Amazon Q in Connect API Reference.

**Amazon Connect Contact Lens provides real-time conversational analytics for chat**

Contact Lens provides real-time conversational analytics for chat, extending the machine learning-powered post-contact analytics (for example, sentiment analysis, automated contact categorization, and more) to real-time contact scenarios. These capabilities enable contact center managers to help detect customer issues during in-progress chat contacts, and help them resolve customer issues faster. For example, managers can now get a real-time email alert when customer sentiment for a chat contact turns negative, allowing them to join the in-progress contact and help resolve the customer issue.

For more information, see Analyze conversations using conversational analytics. In addition, see the ListRealtimeContactAnalysisSegmentsV2 action in the Amazon Connect API Reference.

**Amazon Connect Contact Lens provides generative AI–powered contact summarization (Preview)**

Contact Lens provides generative AI–powered post-contact summarization, enabling contact center managers to more efficiently monitor and help improve contact quality and agent performance.

Contact Lens already labels parts of contact transcripts as issue, outcome, and action item. With this launch, Contact Lens will now condense a long customer conversation into a concise and coherent summary (for example, customer didn't receive reimbursement for last minute flight cancellation, and the agent didn't offer partial reimbursement as per the SOP). This enables managers to help reduce the overall time spent on evaluating contact quality and agent performance, as they no longer have to read long contact transcripts or listen to call recordings.

For more information, see View post-contact summarization powered by generative AI (Preview).
Amazon Connect supports in-app, web, and video calling

The Amazon Connect in-app, web, and video calling capabilities enable your customers to contact you without ever leaving your web or mobile application. You can use these capabilities to pass contextual information to Amazon Connect. This enables you to personalize the customer experience based on attributes such as the customer's profile or other information, like actions previously taken within the app.

For more information, see Set up in-app, web, and video calling capabilities. In addition, see the StartWebRTCContact action in the Amazon Connect API Reference.

Amazon Connect supports two-way SMS

Amazon Connect supports two-way Short Messaging Service (SMS) capabilities, making it easy for you to resolve customer issues by text messaging. SMS offers a ubiquitous and convenient channel for customers to get help, while enabling you to deliver personalized experiences at a lower cost.

To get started, claim your two-way SMS number from Amazon Pinpoint SMS and associate the number with your Amazon Connect instance. Amazon Connect SMS uses the same automation, routing, configuration, analytics, and agent experience as calls and chats, making it easy to deliver seamless omnichannel customer experiences.

For more information, see Set up SMS messaging. In addition, see the following new actions in the Amazon Connect API Reference Guide.

- AssociateFlow
- DisassociateFlow
- GetFlowAssociation
- ImportPhoneNumber
- ListFlowAssociations
- SendChatIntegrationEvent

Analytics data lake (Preview)

You can use Analytics data lake as a central location to query various types of data from Amazon Connect. This data includes contact records and Contact Lens conversational analytics. Data is
refreshed around every 24 hours. You can use the Analytics data lake to create custom reports or run SQL queries.

For more information, see Access Analytics data lake. In addition, see new actions in the Analytics data lake actions topic in the Amazon Connect API Reference.

### Added metrics to the GetMetricDataV2 action

Added metrics to the GetMetricDataV2 action. For example: AGENT_ANSWER_RATE, AGENT_NON_ADHERENT_TIME, CONTACTS_ON_HOLD_AGENT_DISCONNECT, CONTACTS_ON_HOLD_CUSTOMER_DISCONNECT, SUM_AFTER_CONTACT_WORK_TIME, SUM_CONNECTING_TIME_AGENT, and more. Added Non-Adherent time to the historical metrics report in AWS Regions where Forecasting, capacity planning, and scheduling is available.

### Customer Profiles block enhancements

You can access more customer information, including orders, cases, assets, custom attributes, and calculated attributes through the Customer Profiles Flow block. For more information, see Flow block: Customer profiles.

### View and manage applied service quotas for Amazon Connect using AWS Service Quotas

Service Quotas allows you to view both default and applied quota values for resources used by each of your Amazon Connect instances. When requesting a quota increase, Service Quotas allows you to indicate both the Amazon Connect quota and desired value. For quotas that support resource level adjustability you can also specify your Amazon Connect instance. For more information, see Amazon Connect service quotas.

### Added an action to AmazonConnectServiceLinkedRolePolicy

Updated AmazonConnectServiceLinkedRolePolicy with an action for Amazon Q in Connect. For a description of the additional action, see Amazon Connect updates to AWS managed policies.

### Amazon Connect now provides a Contact Lens conversational analytics dashboard

Amazon Connect now provides a pre-built Contact Lens conversational analytics dashboard that enables customers to understand why customers are contacting, the trends of contact drivers over
time, and the performance of each of those call drivers (e.g., average handle time for call driver “where’s my stuff?”). For more information, see Contact Lens conversational analytics dashboard.

Amazon Connect now provides a pre-built queue performance dashboard

Amazon Connect now provides a pre-built queue performance dashboard that helps contact center managers analyze, track, and improve contact center performance. This dashboard enables managers to view and compare real-time and historical aggregated queue performance using custom-defined time periods (e.g., week over week), a summary chart, and a time series graph. For more information, see Queue performance dashboard.

Amazon Connect prompts configuration page provides CloudTrail coverage

The prompts configuration user interface has been updated to make it more efficient for you to manage prompts. In addition, when you add, update or delete a prompt from the Amazon Connect admin website, a record of that activity is available in AWS CloudTrail for visibility, reporting, and compliance. For example, you may notice a discrepancy in the IVR prompt that customers hear when they call your support line. To investigate, you can leverage AWS CloudTrail to answer questions such as, "who saved this recording?" and "when was this prompt changed?" For more information about the new prompts page, see Create prompts.

Amazon Connect enables integration with your preferred file scanning application to detect malware

You can integrate Amazon Connect with your preferred file scanning application to detect malware or other unwanted content in attachments before they can be shared in a chat or uploaded to a case. This capability provides an additional layer of protection for your customers and organization by preventing malicious files from being shared and downloaded. For more information, see Set up attachment scanning.

Amazon Connect outbound campaigns voice dialing API

You can create contacts for all high-volume voice outreach by using the BatchPutContact API. This API makes it easier for you to track outcomes of all campaign calls by using the Amazon Connect contact record.
Amazon Connect Cases supports author name on comments

You can programmatically add and view author comments by using the `CreateRelatedItem` and `SearchRelatedItems` APIs.

Updated `AmazonConnectCampaignsServiceLinkedRolePolicy` service-linked role managed policy

Updated the service-linked role managed policy for outbound campaigns. For a description of the additional actions, see [Amazon Connect updates to AWS managed policies](#).

Added Create persistent chat association flow block and `CreatePersistentContactAssociation` API

You can set up a chat to be persistent either when the chat session is initially created or at any time during the lifetime of the chat. To set up persistent chat after the chat session has started, use the new `CreatePersistentContactAssociation` API or include the new [Create persistent contact association](#) block in your flow.

Optimization to how the CCP detects and handles stale WebSocket connections

When an agent initializes the CCP, a WebSocket connection is opened and it is used during subsequent contact handling. If that agent experiences poor network conditions, this may result in the agent becoming unreachable without the backend detecting it. With this release the WebSocket connections for these agents are detected as stale and cleaned in 1-2 minutes.

Amazon Connect can now identify, within about 2 minutes, a situation where a chat customer and an agent are on a chat contact, and the agent becomes unreachable (for example, as a result of losing wifi or losing power to their local machine), allowing the backend to run the chat disconnect flow. Before this optimization, it could take up to 10 minutes to run any chat disconnect flows.

Added new service-linked role policy and service-linked role

Added `AmazonConnectSynchronizationServiceRolePolicy` service-linked role policy and `AWSServiceRoleForAmazonConnectSynchronization` service-linked role for managed synchronization. The policy and role provide access to read, create, update, and delete Amazon Connect resources and is used to automatically synchronize AWS resources across AWS regions. For
Added Contact Lens conversational analytics metrics to the GetMetricDataV2 API

You can analyze aggregate agent and contact performance using Contact Lens conversational analytics metrics in the GetMetricDataV2. The following new metrics were added: non-talk time percent, talk time percent, talk time agent percent, and talk time customer percent. For descriptions of these metrics, see Historical metrics definitions.

Added configuration management across AWS Regions for Amazon Connect Global Resiliency customers

Amazon Connect Global Resiliency customers can use the ReplicateInstance API to copy configuration information for resources such as users, routing profiles, queues, and flows across AWS Regions. The API also automatically matches the service quotas for these resources across AWS Regions as part of the replication process. For more information, see Create a replica of your existing Amazon Connect instance.

Added the BatchGetFlowAssociation API. Use this API to obtain a list of flow-associations for the resource identifiers provided in the API request. For example, you can list which phone numbers are associated with which flows in an Amazon Connect instance.

October 2023 Updates

Added actions to AmazonConnectServiceLinkedRolePolicy

Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Customer Profiles. For a description of the additional actions, see Amazon Connect updates to AWS managed policies.

Third-party applications preview

You can integrate third-party applications into the agent workspace. For more information, see Third-party applications (3p apps) in the agent workspace (Preview) and the Amazon Connect agent workspace third-party developer guide.
**Added actions to AmazonConnectServiceLinkedRolePolicy**

---

**Note**

In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.

---

Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Wisdom. For a description of the additional actions, see [Amazon Connect updates to AWS managed policies](#).

**Added the UpdatePhoneNumberMetadata API**

Use the [UpdatePhoneNumberMetadata](#) to update the metadata for a phone number, such as the phone number description.

**Add as many as four access control tags to a single security profile**

Adding additional access control tags will make a given security profile more restrictive. For example, if you add four access control tags like BPO:AcmeCorp, Specialty:Claims, Department:Billing, and City:NewYork, the user would only be able to see resources containing all four of these tags. For more information, see [Tag-based access control](#).

**Added actions to AmazonConnectServiceLinkedRolePolicy**

Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Customer Profiles. For a description of the additional actions, see [Amazon Connect updates to AWS managed policies](#).

**CTI Adapter upgrade for third-party cookies**

This upgrade prevents the blocking of third-party cookies from impacting Amazon Connect across Chrome and all supported browsers. For more information, see [Amazon Connect CTI Adapter for Salesforce](#) release notes and [Use Amazon Connect Streams API for third-party cookies](#).
Create and customize up to 15 communications widgets

You can create and customize up to 15 communications widgets per Amazon Connect instance. For more information, see [Add a chat user interface to your website](#).

Access the trailing 90 days of historical agent and contact metrics

You can access the trailing 90 days of historical agent and contact metrics (for example, Service level X, Average handle time) by using the GetMetricDataV2 API. You can also make requests spanning up to 35 days with data categorized by customizable time intervals such as 15 minutes, hourly, or weekly.

In addition, added the following metrics to the GetMetricDataV2 API. These metrics are not available in Amazon Connect admin website.

- Abandonment rate
- Agent non-response without customer abandons
- Average customer hold time all contacts
- Average resolution time
- Contacts resolved in X

Added actions to AmazonConnectServiceLinkedRolePolicy

**Note**

In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.

Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Wisdom. For a description of the additional actions, see [Amazon Connect updates to AWS managed policies](#).
September 2023 Updates

Released Amazon Connect Client Application v1.0.2.38

Released Amazon Connect Client Application v1.0.2.38. This version contains minor fixes and improvements. For more information, see Amazon Connect Client Application.

Added "View my contacts" permission

Added a new security profile permission: View my contacts. On the Contact search page, agents who have this permission can access the contacts that they've handled. If you're using Contact Lens, agents can also review the analyzed recording and transcripts of the contact. For more information, see Security profile permissions for Contact Lens.

Streams API upgrade for third-party cookies

This upgrade prevents the blocking of third-party cookies from impacting Amazon Connect across Chrome and all supported browsers. For more information, see Use Amazon Connect Streams API for third-party cookies.

Create alerts on real-time metrics

You can create rules that automatically send emails or tasks to managers based on the values of real-time metrics. This enables you to alert managers on contact center operations that could potentially impact the end-customer experience.

For more information, see Create alerts on real-time metrics.

"Maximum contacts in queue" includes all channels

If you have a queue that combines more than one channel, and you set a custom value for Maximum contacts in queue, the queue stops accepting new contacts after that number is reached, regardless of the distribution of contacts. For example, if you set the value to 50, and the first 50 contacts are chats, then voice calls are not routed to this queue.

For more information, see Set the Maximum contacts in queue limit.
Manage contacts from the Contact details page

On the Contact details page of an in-progress contact, you can manage a contact by transferring, rescheduling, or ending the contact. For more information, see Manage contacts from the Contact details page.

Upload file attachments to cases

Agents can upload file attachments to cases. For more information, see Enable attachments to share files using chat and upload files to cases. For a list of supported file types, see Amazon Connect feature specifications.

In addition, when agents leave comments on cases, their name is now included.

Search for in-progress contacts

You can search for in-progress contacts on the Contact search page. For more information, see Search for in-progress contacts.

Subscribe to the Contact Data Updated event in the contact event stream

You can subscribe to an event type called CONTACT_DATA_UPDATED. The Contact object includes an UpdatedProperties field. This enables you to monitor for changes to scheduled timestamp for tasks, and changes to user-defined attributes on the contact record. In addition, hierarchy groups information in the AgentInfo object is included for CONTACT_DATA_UPDATED, CONNECTED_TO_AGENT, and DISCONNECTED event types. For more information, see Contact events data model.

APIs to programmatically configure views in step-by-step guides

Amazon Connect provides APIs to programmatically create and manage view resources used in step-by-step guides. View resources define what gets displayed in your agent’s UI during a step-by-step guide. For more information, see the View resource documentation.

Support for UIFN in more than 60 countries

Amazon Connect supports Universal International Freephone number (UIFN) in more than 60 countries that are registered with the International Telecommunications Union, an organization
that supports the administration of the UIFN service. Amazon Connect allows you to enable UIFNs in as many countries as you need, with a requirement of at least 5 countries. For more information, see [UIFN service](#).

**August 2023 Updates**

**Voice dialing for outbound campaigns, no agents required**

You can use Amazon Connect outbound campaigns for high-volume outreach with no agents required. A new dialer type called "Agentless" makes it easier to proactively communicate with your customers for use cases such as personalized voice notifications and appointment reminders. For more information, see [Create an outbound campaign](#) and the [CreateCampaign](#) API.

**Amazon Connect Cases supports nine additional languages**

Amazon Connect Cases supports nine additional languages. You can view the Amazon Connect Cases user interface in any language supported by Amazon Connect regardless of your AWS Region. For more information, see [Amazon Connect Cases](#).

**Granular access controls using resource tags for the agent activity audit report**

You can apply granular permissions to the agent activity audit report in the Amazon Connect historical metrics UI using resource tagging and tag-based access controls. For more information, see [Agent activity audit tag-based access control](#) and [Tag-based access control](#).

**Enhanced user bulk edit**

You can now update up to 100 user records on the Amazon Connect admin website in less than half the time it used to take to make bulk updates. This enhancement is especially useful during contact surges when you may need to change the routing profile for many agents. For more information, see [Edit users in bulk](#).

**Amazon Connect scheduling supports agent group activities**

Amazon Connect scheduling allows contact center managers to more efficiently create and manage activities for groups of agents. For more information, see [Add shift activities in draft or published schedules](#).
GA for global sign-in and agent distribution capabilities

Released the following Amazon Connect Global Resiliency capabilities for general availability: global sign-in and agent distribution across Amazon Connect Regions. This release includes:

- A global sign-in endpoint that enables agents to sign in once and be logged into multiple AWS Regions. This eliminates the need to log off / log back into either region separately.
- An API action to provision agents that are "global" and available in both Regions.
- An API action to distribute agents across these AWS Regions by percentage in 10% increments (for example, 100% in US East (N. Virginia) and 0% in US West (Oregon), or 50% in each Region). This provides you with the flexibility to slowly shift agents across Regions or all at the same time.
- Custom and embedded Contact Control Panel enhancements that enable agents to process contacts from their current active Region without needing to know which Region is active at any given time.

For more information, see Set up your agent's experience with Amazon Connect Global Resiliency. Also see the following new APIs:

- AssociateTrafficDistributionGroupUser
- DisassociateTrafficDistributionGroupUser
- ListTrafficDistributionGroupUsers

Updated UpdateTrafficDistribution with SignInConfig and AgentConfig parameters.

To create a CloudFormation template for traffic distribution groups, see the following topic:

- AWS::Connect::TrafficDistributionGroup

100 rows on real-time metrics tables

You can now view up to 100 rows in the real-time metrics tables on the Real-time metrics page. Previously, the maximum was 50 rows. For more information about real-time metrics, see Real-time metrics reports.
Sorting on column header names

You now have the ability to sort by choosing a column header, rather than choosing the smaller arrow next to the header text. For more information about real-time metrics, see Real-time metrics reports.

Route based on time since last inbound contact

Added an option to specify that selected agents with this routing profile will not have their routing order impacted by outbound contacts. For more information, see Create a routing profile.

July 2023 Updates

Customize the names of flow blocks

To help you distinguish blocks in a flow, you can customize the names of blocks. For example, you might rename a Play Prompt flow block to Welcome message or a Get customer input flow block to Hotel booking Lex bot. The following GIF shows how to customize the name of a flow block.

For more information, see Customize the name of a block.

Archive, restore, and delete flows and modules

You can archive, restore, and delete flows and modules by using the Amazon Connect admin website. This makes it easier to manage flows and modules that are not in use or no longer needed.
For example, flows used only during certain times of the year can be archived when not in use and then unarchived when needed. When a flow or module has been archived, you can then permanently delete it so it is no longer available within your list of flows and modules. For more information, see Archive, delete, and restore flows.

**Undo and redo actions in the flow designer**

You can undo and redo actions in the flow designer. Choose the undo and redo items on the toolbar. Or, with your cursor on the flow designer canvas, use the shortcut keys: Ctrl+Z to undo, Ctrl+Y to redo. For more information, see Undo and redo actions in the flow designer.

**Add notes to a flow block**

To add notes to a block, on the toolbar choose Annotation. Or, with your cursor on the flow designer canvas, use the shortcut keys: Ctrl + Alt +N. A yellow box opens for you to type up to 1000 characters. This enables you to leave comments that others can view. For more information, see Add notes to a block.

The following GIF shows how to move notes around the flow designer and attach them to a block.
Use the mini-map to navigate a flow

On the flow designer, the mini-map view helps you easily navigate the flow. The drag-to-move mini-map has visual highlights that enable you to quickly move to any point in the flow. For more information, see Use the mini-map to navigate a flow.

The following GIF shows an example of how you can use the mini-map to navigate a large flow.

Restrict attributes to specific flows

Released a new type of attributes called a flow attribute. Flow attributes are restricted to the flow in which they are configured. They are useful in situations where you don't want to persist the data throughout the contact, such as when you need to use sensitive information like the customer's credit card number to do a Lambda data dip. For more information, see Flow attributes.

Import time off balances

You can import time off balances for your users. You can also set the group allowance for time off by hour, for each calendar day, for specific time off activities. Amazon Connect uses the time off balance to automatically approve or decline time off requests based on the agent's available net balance and the group allowance for time off. For more information, see Import an agent's time off balance in a .csv file and Set group allowance for time off.
Schedule flexible days and shift activities based on shift length

The following scheduling functionality has been released:

- You can generate agent schedules that have the appropriate number of activities, such as breaks or meals, depending on the duration of the shift. The required number of breaks and meals are automatically placed in schedules that are compliant to various regional labor laws.

- You can generate agent schedules that include flexible days, that is, days that will be optionally scheduled if there's a need. Amazon Connect can automatically generate flexible schedules that are compliant to agent's contracts and regional labor laws, thereby saving time for schedulers.

For more information, see Create shift profiles.

Amazon Connect Customer Profiles supports rule-based matching and merging

Amazon Connect Customer Profiles supports rule-based resolution to match and merge similar profiles into unified ones. This enables you to enhance customer service by granting agents and automated systems access to relevant customer information. As a result, interactions become faster and more personalized for customers. For more information, see Use Identity Resolution to consolidate similar profiles.

Released Amazon Connect Client Application v1.0.1.33

The Amazon Connect Client Application is used to record agent screens. With this newer version you no longer need to restart your desktop after installing the client application. For the download location, see the Amazon Connect Client Application topic.

Amazon Connect Cases provides case assignment

Case assignment helps organizations reduce the time to resolve customer issues by clearly tracking case activities and resolution ownership. Agents can associate a case with a queue or an individual agent for resolution. Agents can view and filter cases assigned to their queue, and managers can directly assign cases to individual agents. For more information, see Set up case assignment.
Contact Lens Conversational Analytics metrics in the API

You can analyze aggregate agent and contact performance using Contact Lens Conversational Analytics metrics in the `GetMetricDataV2` API. The list of metrics include Average contact duration, Average conversation duration, Average greeting time agent, Average holds, Average interruptions agent, Average interruption time agent, Average non-talk time, Average talk time, Average talk time agent, and Average talk time customer. For more information, see Historical metrics definitions and `GetMetricDataV2`.

Amazon Connect Wisdom supports real-time recommendations for chat conversations

**Note**

In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.

Amazon Connect Wisdom delivers ML-powered, real-time recommended information to help chat agents quickly solve customer needs.

Delete queues and routing profiles programmatically

You can delete queues and routing profiles programmatically. For more information, see the following topics:

- [DeleteQueue](#) action
- [delete-queue](#) AWS CLI
- [DeleteRoutingProfile](#) action
- [delete-routing-profile](#) AWS CLI

To create an AWS CloudFormation template for queues and routing profiles, see the following topics:

- [AWS::Connect::Queue](#)
June 2023 Updates

Agents can change their audio device settings in the CCP and agent workspace

You can configure the Contact Control Panel (CCP) or agent workspace to enable agents to select their preferred device for microphone input and audio output, such as voice media and new contact notifications. For more information, see How to use the CCP to change your audio device settings.

Amazon Connect Chat: New interactive message types

Amazon Connect Chat supports new interactive message types: quick replies and carousels. With quick replies, customers are presented with a list of response options (for example, Yes, No) that they can easily click to reply. Carousels present a set of interactive messages in a horizontally-scrolling format. Your customers can scroll through them and select the best option. For more information, see Add interactive messages to chat.

GetMetricDataV2 API: Region availability and new functionality

The GetMetricDataV2 API is available in the AWS GovCloud (US-West) Region. GetMetricDataV2 is now released in all AWS Regions where Amazon Connect is offered. This API enables you to access the trailing 35 days of historical agent and contact metrics (for example, service level, average handle time) with customizable filters and groupings.

You can use GetMetricDataV2 to build custom dashboards to measure queue and agent performance over time. For example, you can identify the number of contacts that were disconnected by an agent versus disconnected by a customer hanging up. For more information, see GetMetricDataV2.

Search for existing tags within an Amazon Connect instance

Amazon Connect provides the ability to search for existing tags within an instance, both programmatically via API and within the UI. When tagging resources, you can search from pre-existing key:value pairs before creating new ones. For more information, see the SearchResourceTags API.
Added screen recording capabilities to Contact Lens

Amazon Connect Contact Lens provides screen recording capabilities, making it easy for you to help agents improve their performance. With screen recording, you can identify areas for agent coaching (for example, long contact handle duration or non-compliance with business processes) by not only listening to customer calls or reviewing chat transcripts, but also watching the agent's actions while they are handling a contact. For more information, see Set up and review agent screen recordings.

Amazon Connect scheduling allows agents to manage time off requests

Amazon Connect scheduling allows contact center agents to manage their time off requests in a self-serve manner. For more information, see Create a time off request.

Real-time data export of unified customer profiles to an Amazon Kinesis Data Stream

Amazon Connect Customer Profiles supports real-time data export of unified customer profiles to an Amazon Kinesis Data Stream. Companies can enable data streaming and automatically receive data for new profiles and updates to existing profiles into their Amazon Kinesis Data Stream. For more information, see Set up real-time export.

May 2023 Updates

Added theme detection to Contact Lens

Contact Lens provides a machine learning powered capability for businesses to help identify top contact drivers by grouping customer conversations into themes. For more information, see Use theme detection to discover issues.

New APIs for managing prompts

You can programmatically create and manage prompts using APIs, for example, to extract prompts stored in Amazon Connect and add them to your Amazon S3 bucket. AWS CloudTrail, AWS CloudFormation, and tagging are supported. For more information, see Prompt actions in the Amazon Connect API Reference Guide. Also see AWS::Connect::Prompt in the AWS CloudFormation User Guide.
**Added supervisor alerts on agent performance**

Amazon Connect Contact Lens provides supervisor alerts on agent performance. This enables you to identify which contacts (for example, those with an evaluation score less < 50%) that require supervisors follow-up with agents on their team. For more information, see [Create supervisor alerts on agent performance](#).

**Interactive messages: Rich formatting in chat titles and subtitles**

You can add rich formatting to the titles and subtitles of your chat messages. For example, you can add links, italics, bold, numbered lists, and bulleted lists. You use [markdown](#) to format your text. For more information, see [Rich formatting in titles and subtitles](#) in the Add interactive messages to chat topic.

**April 2023 Updates**

**GA for Amazon Connect evaluation capabilities**

Released Amazon Connect evaluation capabilities for general availability. Use these capabilities to:

- [Create evaluation forms](#)
- [Evaluate agent performance](#)
- [Create rules](#) that trigger an action (such as send email or tasks) based on evaluation results
- [Search evaluation forms and evaluations](#)

To manage evaluation forms programmatically, see the [Evaluation actions in the Amazon Connect API Reference](#). To create a shared template for evaluation forms, see the AWS::Connect::EvaluationForm resource in the [AWS CloudFormation User Guide](#).

**New API: Use CreateParticipant to customize chat flow experiences**

Added the [CreateParticipant](#) API which you can use to customize chat flow experiences. You use it to integrate custom participants. For more information, see [Customize chat flow experiences by integrating custom participants](#).
Customer Profiles displays case information in the agent workspace

Using Amazon Connect Customer Profiles inside the agent workspace, agents can see cases from third-party case management solutions and Amazon Connect Cases inside a particular customer profile. For more information, see Use Customer Profiles and Access Customer Profiles in the agent workspace.

Added Cross-channel concurrency

You can configure an agent's routing profile to receive contacts from multiple channels at the same time. For example, while an agent is on a voice contact, they can be offered contacts from any other channels enabled in the routing profile, such as chats and tasks.

For more information, see Create a routing profile. Also see the CrossChannelBehavior API.

Set Voice ID block supports fraud watchlist ID

Updated the Set Voice ID block so it supports fraud watchlist ID for fraud detection.

Search, sort, and filter published agent schedules

Schedulers can quickly search, sort, and filter agent schedules from within the published schedule calendar. For more information, see How supervisors view published schedules.

March 2023 Updates

Added Wisdom support for Microsoft SharePoint Online

Note

In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.

You can choose Microsoft SharePoint Online as knowledge base for Wisdom articles. For more information, see Enable Amazon Q in Connect for your instance. Also see the AppIntegrationsConfiguration API in the Amazon Q in Connect API Reference.
Create step-by-step guides for your agents

Inside the out-of-the-box Amazon Connect agent workspace, you can create workflows that walk agents through custom UI pages that suggest what to do at a given moment during a customer interaction. You can create guides that help agents identify customer issues and recommend subsequent actions, as well as surface screen-pops and forms for submitting transactions and disposition codes. For more information, see Step-by-step Guides.

Added support for nested JSON in Invoke AWS Lambda function flow block

The Invoke AWS Lambda function flow block supports JSON responses. For more information, see Flow block: Invoke AWS Lambda function.

Added Show View flow block

This block is used to configure UI based workflows that you can surface to users in front end applications. For more information, see Flow block: Show view.

Added staff level shift profile

You can assign a shift profile to individual agents. This is useful to do when, for example, you have part-time agents who are in the same staffing group as your full-time agents, but they require their own shift profile. For more information, see the Associate to shift profile option described in Create staff rules for scheduling.

Added support for multiple fraudster watchlists

Every domain has a default watchlist where all existing fraudsters are placed by default. You can create and manage custom watchlists to be evaluated against for known fraudster detection. For more information, see Known fraudster detection, and see new actions in the Amazon Connect Voice ID API Reference.

Search and sort schedules in the Schedule Manager

Schedulers can quickly search for schedule names using partial keywords or sort the schedule list based on start date, end date, creation date, or updated date. For more information, see Search and sort a schedule.
Added the ability to configure multiple IAM roles that can be assigned to a single user when using SAML 2.0

You can configure multiple IAM roles that can be assigned to a single user when using SAML 2.0 which enables you to support user access from multiple identity providers simultaneously. For example, if you are migrating identity providers, you can configure multiple IAM roles associated to a single user and that user will be able to access Amazon Connect from either provider. To learn more about configuring IAM roles for SAML 2.0 in Amazon Connect, see the Configure SAML with IAM for Amazon Connect documentation.

Added panel template for interactive chat messages

With a panel template, you can present customers with up to 10 choices under one question in a chat message. For more information, see Add interactive messages to chat.

Added GetMetricDataV2 API

Added the GetMetricDataV2 API to the Amazon Connect API Reference Guide. This API enables you to programmatically access trailing 14 days of historical agent and contact metrics data. It extends the capabilities of the GetMetricData API, provides new historical metrics (for example, the number of contacts disconnected, and the number of callback attempts), and provides the ability to filter metrics with more granularity.

February 2023 Updates

Added new attribute type ENHANCED_CONTACT_MONITORING to Describe, List and Update Instance Attribute APIs

This release updates the APIs: DescribeInstanceAttribute, ListInstanceAttributes, and UpdateInstanceAttribute. You can use it to programmatically enable/disable enhanced contact monitoring using attribute type ENHANCED_CONTACT_MONITORING on the specified Amazon Connect instance. For more information, see DescribeInstanceAttribute, ListInstanceAttributes, and UpdateInstanceAttribute.

Added the DeleteDomain API for Cases

For more information, see the DeleteDomain API in the Amazon Connect Cases API Reference Guide.
Added RelatedContactId to StartTaskContact API

You can link together an unlimited number of task contacts using the RelatedContactID parameter supported in the StartTaskContact API. For more information, see Linked tasks and the StartTaskContact API in the Amazon Connect API Reference Guide.

Amazon Connect Cases integrates with AWS PrivateLink

For more information, see Creating an interface VPC endpoint for Amazon Connect.

Added support for more granular access controls (using resource tags) to view real-time metrics for agents, queues, and routing profiles

You can enable more granular access controls for real-time metrics by configuring resource tags and access control tags within security profiles in the Amazon Connect admin website. For more information, see Real-time tag-based access control and Tag based access control in Amazon Connect.

Added support to provide more granular permissions to metrics reports, including new permissions for real-time metrics, historical metrics, and agent activity audit

You can configure more granular permissions to metrics and reports from within security profiles in the Amazon Connect admin website. For more information, see Permissions required to view real-time metrics reports and Agent activity audit permissions.

Added support to provide visibility into an agent’s next activity

You can view an agent's next activity in the real-time metrics agent table in the Amazon Connect real-time metrics UI and by using the public API. For more information, see the NextStatus API reference.

Apply S3 Object Lock for the call recordings bucket

You can use Amazon S3 Object Lock in combination with your call recording bucket to help prevent call recordings from being deleted or overwritten for a fixed amount of time, or indefinitely. For more information, see How to set up S3 Object Lock for immutable call recordings.
CloudFormation templates for instance management

You can use CloudFormation templates to manage Amazon Connect instances for associating Amazon Lex and Lex V2 bots, Lambda functions, security keys, and approved origins—along with the rest of your AWS infrastructure—in a secure, efficient, and repeatable way. For more information, see Amazon Connect resource type reference in the AWS CloudFormation User Guide.

January 2023 Updates

Added long lasting, persistent chat experiences

Amazon Connect makes it easier for you to deliver long lasting, persistent chat experiences for your customers. Persistent chats enable customers to resume previous conversations with the context, metadata, and transcripts carried over, eliminating the need for customers to repeat themselves and allowing agents to provide personalized service with access to the entire conversation history. To set up persistent chat experiences, provide a previous contact ID when calling the StartChatContact API to create a new chat contact.

For more information, see Enable persistent chat. Also see changes to StartChatContact in the Amazon Connect API Reference Guide, and see the new RelatedContactId parameter in the GetTranscript API in the Amazon Connect Participant Service API Reference Guide.

December 2022 Updates

Added message receipts feature for chat messages

The message receipts feature allows customers to receive Message delivered and Read receipts after they send a chat message. For more information, see Enable message Delivered and Read receipts in your chat user interface. Also see the SendEvent action, and the Item, MessageMetadata, and Receipt data types in the Amazon Connect Participant Service API Reference Guide.

Updates to GetCurrentMetricData and GetCurrentUserData

For the GetCurrentMetricData API, added support for routing profile filter, sort criteria, and grouping by routing profiles. For the GetCurrentUserData API, added support for routing profiles, user hierarchy groups, and agents as filters, and next status and agent status name. For both APIs, added ApproximateTotalCount.
Added chat timeouts for chat participants

When a chat conversation between an agent and a customer has been inactive (no messages sent) for a certain amount of time, you may want to consider a chat participant to be idle, and you may even want to automatically disconnect an agent from the chat. To set up chat timeout timers, see Set up chat timeouts for chat participants.

Microsoft Edge Chromium support

Amazon Connect now supports Microsoft Edge Chromium. For more information about supported browsers, see Browsers supported by Amazon Connect.

Amazon Connect supports JSON as a content type for chat messages

By supporting JSON as a content type, Amazon Connect provides you with a way to pass additional information over chat to provide rich personalized experiences. For example, rendering updates to a custom UI, customer-built interactive messages, language translation capabilities, and passing customer metadata to a third party bot. For more information, see StartChatContact in the Amazon Connect API Reference Guide, and SendMessage in the Amazon Connect Participant Service API Reference Guide.

Added topic on Amazon Connect availability by Region

For more information, see Availability of Amazon Connect services by Region.

Contact Lens granular data redaction

When you set up Contact Lens sensitive data redaction, you can choose which entities you want to redact, and how you want the redaction to appear in the transcript. For more information, see Enable redaction of sensitive data.

Additional Contact Lens language support and Region availability

Contact Lens now supports the following languages: English - New Zealand, English - South Africa. It is also available in the following Regions: Africa (Cape Town), Asia Pacific (Seoul), Asia Pacific (Singapore).
Released Barge to allow contact center managers to join ongoing calls

Barge allows managers to join and participate in an ongoing customer service call between a contact center agent and customer. After joining the call, a manager can speak with the customer, add participants, and even choose to remove an agent if needed. For more information, see Barge live conversations.

Added user hierarchy to bulk user upload

You can assign the user hierarchy in the .csv file when you add users in bulk. For more information, see Add users in bulk.

Granular access controls using resource tags for users, security profiles, routing profiles, and queues

You can now enable more granular access controls for security profiles, users, routing profiles, and queues by configuring resource tags within the Amazon Connect console. You can add resource tags to filter and organize these resources logically, and configure access control tags within security profiles to enforce granular permissions. For more information, see Tagging resources in Amazon Connect and Tag based access controls in Amazon Connect.

Bulk user import now includes agent hierarchy and tags

Amazon Connect now allows you to configure hierarchies and resource tags for users in bulk. You can now assign agent hierarchies and resource tags to each agent using the CSV bulk upload template which is available on the user management page. For more information, see Tagging resources in Amazon Connect.

Released Rules Function language

The Rules Function language is a JSON-based representation of a series of rule conditions. Use it to programmatically add conditions to rules. For more information, see Amazon Connect Rules Function language in the Amazon Connect API Reference Guide.

GA for Rules APIs

Released a set of Rules APIs that enable you to programmatically create and manage rules. For more information, see Rules actions in the Amazon Connect API Reference.
Search contacts by agent's first or last name is available in AWS GovCloud

November 2022 Updates

Create step-by-step guides for your agents

Inside the out-of-the-box Connect agent workspace, you can now create workflows that walk agents through custom UI pages that suggest what to do at a given moment during a customer interaction. You can create guides that help agents identify customer issues and recommend subsequent actions, as well as surface screen-pops and forms for submitting transactions and disposition codes. For more information, see Agent Workspace guided experience.

GA for Forecasting, capacity planning, and scheduling

Amazon Connect provides a set of services powered by machine learning that help you optimize your contact center by offering the following:

- Forecasting. Analyze and predict contact volume based on historical data.
- Scheduling. Generate agent schedules for day-to-day workloads that are flexible, and meet business and compliance requirements.
- Capacity planning. Predict how many agents your contact center will require.

For more information, see Forecasting, capacity planning, and scheduling.

Released Contact Lens evaluation forms for preview

You can create evaluation forms, and then make them available to managers to review conversations alongside contact details, recordings, transcripts, and summaries, without the need to switch applications. Conversational analytics automatically pre-populates evaluation scores for criteria like script adherence, sensitive data collection, and customer greetings. For more information, see Evaluate performance (Preview).
Released Contact Lens conversational analytics capabilities for Amazon Connect chat

Amazon Connect Contact Lens provides conversational analytics capabilities for Amazon Connect chat, extending the machine learning powered analytics to better assess chat contacts. For more information, see Analyze conversations using Amazon Connect Contact Lens.

Added configurable Lex timeouts in chat

You can configure how long to wait for a response from a customer in a chatbot conversation before the session expires. For more information, see Configurable time-outs for chat input in the Get customer input topic.

Create rules that send email notifications

You can create Contact Lens rules that send email notifications to people in your organization. For more information, see Create Contact Lens rules that send email notifications.

Added MonitorContact API

Added a new API for programmatically initiating monitoring of ongoing contacts. For more information, see MonitorContact API.

Manage saved reports (admin)

You can view and delete all saved reports in your instance, including reports that were not created by you or that are not currently published. For more information, see Manage saved reports (admin).

Search for profiles using multiple search keys

In addition to searching for profiles with a single search key (i.e., a key-values(s) pair), the SearchProfiles API has been enhanced to support searching for profiles using multiple keys and logical operators. This new functionality allows you to use between 1 and 5 search keys with AND or OR logic to find profiles with attributes that match the search criteria. For more information, see the SearchProfiles API reference.
Delete quick connects using the Amazon Connect console

In addition to deleting quick connects programmatically, you can now delete them using the Amazon Connect console. For more information, see Delete quick connects.

Added DismissUserContact API

Added a new API for programmatically clearing the notifications agents receive after they have missed or rejected a contact, making them eligible to be routed new contacts. This API can also be used to clear similar notifications when an agent encounters an error with accepting the contact or is handling After Contact Work. For more information, see the DismissUserContact API reference.

October 2022 Updates

Add secondary email address and mobile number to user accounts

For more information, see Add users to Amazon Connect.

Emojis for chat messages

Added support for emojis for your customer's chat experience. Agents and customers can now send emojis when composing a chat message, enabling them to visually convey sentiment or emphasis during a chat conversation. For more information, see Enable text formatting for your customer's chat experience.

Released support for Enhanced 911 (E911)

Enhanced 911 (E911) enables location information to be sent to 911 dispatch when a 911 call is placed. In addition to connecting a user with 911 emergency services, customers in the United States can build E911 capabilities to automatically provide the caller's address information to 911 dispatchers. For more information, see Set up US emergency calling in Amazon Connect.

GA for Amazon Connect Global Resiliency

Released Amazon Connect Global Resiliency for General Availability. Global Resiliency enables you to provide customer service anywhere in the world with the highest reliability, performance, and efficiency, while meeting international regulatory requirements. For more information, see Set up Amazon Connect Global Resiliency.
Added Ctrl+Shift+F to search flow block titles and metadata

Press Ctrl+Shift+F to display a search box in the flow designer, and then search the block titles and metadata. To hide the search box, go to Settings, Toolbar, and set the toggle.

The following GIF shows how to use the search box to find flow blocks that have attributes in their title. It also shows how to display or hide the search box using the toggle.

Released Amazon Connect Cases for General Availability

Amazon Connect Cases allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see Amazon Connect Cases and Amazon Connect Cases API Reference.
September 2022 Updates

Searching for a contact? Choose from a list of categories

When you search a contact and filter results by Contact Lens categories, you can pick from a list of categories, rather than manually typing the name of a category.

Updated flow designer

We’ve released a number of improvements to the flow designer experience to make building and editing flows easier.

- Updated look and feel of block dock, blocks, and flow designer canvas.
- Import / Export uses a standard flow language so you can interchangeably build flows in APIs or in the UI.
**Important**

To copy and paste flows and blocks in the updated flow designer, the flow must be in the new flow language. To convert a legacy flow into the new format, you have two options:

- Option 1: In the flow designer user interface, opt in to the updated flow designer. Your legacy flows are automatically converted.

- Option 2: Manually **import** a legacy flow using the updated flow designer.

This option is most useful for scenarios where you have stored your flows in JSON offline. For example, for configuration control, you may have flow configurations in an offline data store. To copy a part of that flow and paste it into the updated flow designer, you need to import it into the updated flow designer. The importing process converts it to the new flow language. After that, you can copy and paste within the updated flow designer. If you want to keep using your offline data store as a source of truth, update the flow with the new format.

- You can use **Search** to filter blocks in the block dock.

- Multi-line block metadata allows you to click and expand to see block configurations.
• Color-coded branches and connectors help you distinguish paths.

• Improved zooming.
- Flow/module metadata appears at the bottom of the block dock.
• New, more intuitive categories (Check, Analyze, and Logic) to make it easier to find the blocks you are looking for.
- Updated user interface in the block **Property** pages.
Search for Amazon Connect users by first name, last name, login, and more

You can search for Amazon Connect users by first name, last name, user login, agent hierarchy, security profile, and routing profile. For example, you can search for all Amazon Connect users who have the first name "Jane."
Queue dashboard

You can visualize historical queue data by using time series graphs to help identify patterns, trends, and outliers specifically for Service Level, Contacts Queued, and Average Handle Time. For more information, see Visualize: Queue dashboard.

August 2022 Updates

Contact search: Apply "Match any" or "Match all" to Contact Lens category searches

When you search for contacts, and filter by Contact Lens categories, you can apply Match any or Match all to the search. For example, you can search contacts with both "category A" and "category B," or with either one of the two categories.

Evaluate calls for voice spoofing

Use Voice ID to evaluate calls for voice spoofing. For more information, see Voice spoofing detection and the Amazon Connect Voice ID API Reference.

Added SearchSecurityProfiles API

Added a new API for programmatically searching security profiles. For more information, see https://docs.aws.amazon.com/connect/latest/APIReference/API_SearchSecurityProfiles.html.

Released Schedule Adherence (Preview)

Contact center supervisors or managers track schedule adherence to understand when agents are following the schedule that you have created. This helps ensure you achieve your service level targets, while improving agent productivity and customer satisfaction. For more information, see Schedule Adherence.

July 2022 Updates

Search for contacts by using the agent's first or last name

You can search for contacts using the agent's first or last name. The filter name is Agent.
Search contacts by agent's first or last name

The following image shows the Agent filter, and the option to choose agents by name.

![Agent filter example](image)

Required permissions to "Agent" search filter

To use the Agent filter on the Contact search page, in your Amazon Connect security profile you must have Users - View permissions, as shown in the following image:

![Permissions table](image)

When you have Users - View permissions, on the Contact search page the Agent filter appears, as shown in the following image:
Without User - View permissions, the Agent filter is not visible, and searching contacts by Agent login is not supported, as shown in the following image:

Released updates for rich text format rendering

On the Contact Search and Contact Detail pages, you can now view chat transcripts that have rich text formatting, such as bold or italic font, bullet points, numbered lists, and hyperlinks. For more information about getting started with Amazon Connect Chat, see Set up your customer’s chat experience.

View call transcript using the CCP or agent application

Agents can view call unredacted transcripts in the CCP and agent application. For more information, see View a call transcript during ACW.
June 2022 Updates

Support for Lex intent confidence scores and sentiment analysis

You can further personalize the automated self-service customer experience using Amazon Lex intent confidence scores and sentiment analysis as a branch within your flows. For more information, see the Get customer input block. For a list of new contact attributes, see Amazon Lex contact attributes.

Metrics Updates

The following updates were released in June 2022.

15 minute scheduled reports

You can now schedule historical metrics to refresh every 15 minutes. To select 15-minute schedules, select generate this report Hourly every .25 hours (this is the top most option in the second dropdown), for the previous .25 hours. The following image shows the values that you need to select.
## Filter Real-Time Metrics Agent Table by Agent

You can now filter the agent table on the Real-Time Metrics page by agent. This filter functions the same as the existing queues, routing profiles, and agent hierarchy filters.
New contact transferred related metrics

We are upgrading the existing Contacts transferred in and Contacts transferred out historical metrics to have consistent definitions. We are adding Contacts transferred in by agent and Contacts transferred out by agent for more granular contact transferred related metrics.

Changes to real-time metrics agent tables

We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables are sorted by agent status instead of by agent login.

Additionally, the queues and routing profiles table are sorted by agents online instead of by queue or routing profile name.
Faster reload times for the Real-time metrics page

We are upgrading the performance of the Real-time metrics page so reload times are faster. The page will have the same functionality and user experience as the existing Real-time metrics page.

Released Amazon Connect Cases (Preview)

Amazon Connect Cases (Preview) allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see Amazon Connect Cases (Preview) and Amazon Connect Cases API Reference (Preview).

GA for Amazon Connect outbound campaigns

Released Amazon Connect outbound campaigns, formerly known as High-volume outbound communications. This release includes a set of APIs for creating and managing outbound campaigns. For more information, see Enable Amazon Connect outbound campaigns and Amazon Connect Outbound Campaigns API Reference.

Released GetCurrentUserData API

Released the GetCurrentUserData API. It enables you to return the real-time active user data from the specified Amazon Connect instance.

Released task templates

You can now create custom task templates, making it easy for agents to consistently capture the relevant and required information to create or complete tasks. For more information, see Create task templates. For information about using the API to programmatically create and manage task templates, see the Amazon Connect API Reference and the Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.

New API to transfer contacts

Added a new API that you can use to transfer contacts from one agent or queue to another agent or queue at any point after a contact is created. You can transfer a contact to another queue by providing the flow which orchestrates the contact to the destination queue. This gives you more control over contact handling and helps you adhere to the service level agreement (SLA) guaranteed to your customers.
For information, see TransferContact in the Amazon Connect API Reference.

May 2022 Updates

Updated workflow for outbound campaigns

Updated the workflow for onboarding to outbound campaigns using the Amazon Connect and Amazon Pinpoint user interface. For more information, see Enable outbound campaigns.

Voice ID expires speakers

For BIPA Compliance, Amazon Connect Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years. You can see a speaker's last access time by looking at the lastAccessedAt attribute returned by the DescribeSpeaker and ListSpeakers APIs.

For more information, see What data is stored? in the Use real-time caller authentication with Voice ID topic.

April 2022 Updates

New API to change an agent's current status

Amazon Connect provides an API to programmatically change the current status of an agent. Agent statuses are used to determine when an agent is Available to be routed contacts in Amazon Connect, versus when they are set to Offline or a custom status such as Lunch or Break and should not be routed contacts. For more information, see PutUserStatus in the Amazon Connect API Reference.

New API to search for users by name, agent hierarchies, and tags

Added API to search for user records in your Amazon Connect instance. This new API provides a programmatic and flexible way to search for users by first name, last name, username, routing profile, security profile, agent hierarchies or tags. For example, you can now use this API to search for all users tagged with a Department:key value pair. You can also quickly find a list of all users assigned to a specific security profile, routing profile, or agent hierarchy. For more information, see the Amazon Connect API Reference.
New APIs to claim and configure phone numbers

Added new APIs to claim new phone numbers and configure them programmatically. Using these APIs, you can programmatically search for and claim available phone numbers, associate phone numbers to flows, or release phone numbers that are no longer needed. Additionally, the phone number APIs come with support for AWS CloudFormation. For more information, see the Amazon Connect API Reference and the Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.

Telephony: Multi-party calls

You can enable Amazon Connect to allow up to six parties on a call: the agent, the caller, and four more participants. (By default, Amazon Connect allows agents to have up to three parties on a call: the agent, and caller, and another participant.) For more information, see Update instance settings. For more information, see Host multi-party calls.

For information about new functionality on the existing Connection and Contact API in Amazon Connect Streams, see the Amazon Connect Streams Readme.

The following sections describes how managing multi-party calls differs from managing three-party calls.

Contents

• New behavior with multi-party calls

• Comparison: Three-party and multi-party calls

New behavior with multi-party calls

• All agents see all of the connections in a call.

• All agents have exactly the same capabilities as any other agent on the call. This takes into affect the moment an agent accepts the invitation to join the call.

• Before a warm transfer is complete, an agent can start talking to the caller as well as disconnect any other agent on the call.
Comparison: Three-party and multi-party calls

The following table summarizes the differences between the agent's experience using the Contact Control Panel (CCP) for three-party calls and multi-party calls.

- Primary agent: the first agent on the call.
- Secondary agent: any agent other than the first agent on the call.

<table>
<thead>
<tr>
<th>Three-party calls</th>
<th>Multi-party calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent can control hold, resume, and disconnect only the parties they added.</td>
<td>All agents are have the same call control capabilities.</td>
</tr>
<tr>
<td>Agent can add one other participant to an existing call, for a total of three participants (the agent, the caller, and another participant).</td>
<td>Any agent on the call can add additional participants, as long as the total number of participants on the call, including themselves, does not exceed six.</td>
</tr>
<tr>
<td>Agent can put only the party they added on hold.</td>
<td>Any agent on the call can put any party on hold.</td>
</tr>
<tr>
<td>When a primary agent places a secondary agent on hold, the secondary agent can't take themselves off hold.</td>
<td>Any agent on the call can take themselves off hold.</td>
</tr>
<tr>
<td>Secondary agent can talk to the primary agent during hold.</td>
<td>Secondary agents cannot talk to each other until they are taken off hold.</td>
</tr>
<tr>
<td>Primary agent can only mute themselves.</td>
<td>Any agent on the call can mute any other participant on the call.</td>
</tr>
<tr>
<td>Secondary agent can only mute themselves.</td>
<td></td>
</tr>
<tr>
<td>When an agent disconnects (leaves or is disconnected), call control continues to be available to the remaining agent(s) on the call.</td>
<td>When an agent disconnects, control of the call is transferred to the remaining agents.</td>
</tr>
<tr>
<td>Only the primary agent can disconnect a party on the call. The secondary agent can</td>
<td>All agents have the capability to disconnect any other party.</td>
</tr>
</tbody>
</table>
### Three-party calls vs. Multi-party calls

<table>
<thead>
<tr>
<th>Three-party calls</th>
<th>Multi-party calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect the caller only if the primary agent has disconnected.</td>
<td>All agents can see all connections.</td>
</tr>
<tr>
<td>The primary agent can see two connections (caller and another party), while a secondary agent sees only the transfer connection.</td>
<td>All agents can see all connections.</td>
</tr>
<tr>
<td>An agent only sees <strong>internal transfer</strong> for another agent on the call.</td>
<td>An agent sees the quick connect ID for other agents, instead of just <strong>internal transfer</strong>.</td>
</tr>
<tr>
<td>Not applicable.</td>
<td>When an party is being dialed, an agent on a multi-party call cannot add another party until the prior dial operation is completed (party added or call leg terminated).</td>
</tr>
</tbody>
</table>

---

**Play prompts from an Amazon S3 bucket**

Added the ability to source prompts from an Amazon S3 bucket. You can store as many voice prompts as needed in Amazon S3 and access them in real time by using contact attributes in the following contact blocks that play prompts: **Get customer input**, **Loop prompts**, **Play prompt**, and **Store customer input**.

For more information, see the [Play prompt](#) block. For information about the policy required for Amazon Connect to access the Amazon S3 bucket, see [Set up prompts to play from an S3 bucket](#).

**CloudTrail support for queues and routing profiles**

Amazon Connect records all changes made to users, routing profiles, and queues as events in AWS CloudTrail. For example, you can identify who took which action, what resources were acted upon, and when an event occurred. For more information, see the section called “Logging service API calls”.
March 2022 Updates

Rich messaging for chat

Added support for rich messaging for your customer's chat experience. Agents and customers can use bold, italics, bulleted lists, numbered lists, hyperlinks, and attachments. For more information, see Enable text formatting for your customer's chat experience.

Customer Profiles: Object type mapping user interface

Added a user interface for creating object type mapping by using the Amazon Connect admin console. For more information, see Create an object type mapping.

February 2022 Updates

Added bulk ingestion of data for Customer Profiles

Added support for the bulk ingestion of data for Customer Profiles. For more information, see Bulk ingestion of data in the Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk topic.

New CloudWatch metrics for chat

Added the following Amazon CloudWatch metrics for chat: ConcurrentActiveChats, ConcurrentActiveChatsPercentage, ChatBreachingActiveChatQuota, and SuccessfulChatsPerInterval. For more information, see Monitoring your instance using CloudWatch.

January 2022 Updates

Configure maximum chat duration up to 7 days

You can configure the maximum chat duration to last up to 7 days. For more information, see the ChatDurationInMinutes parameter in the StartChatContact API.

Add custom vocabularies to Contact Lens

Improve the accuracy of speech recognition for product names, brand names, and domain-specific terminology, by expanding and tailoring the vocabulary of the speech-to-text engine in Contact Lens. For more information, see Add custom vocabularies.
Earlier Updates

December 2021 Updates

Communications widgets support browser notifications

The communications widget supports browser notifications for desktop devices. For more information, see Browser notifications.

Ingest data into Customer Profiles from Segment and Shopify

For more information, see Set up integration for Segment and Set up integration for Shopify.

November 2021 Updates

Released unified agent application

Amazon Connect released the unified agent application to improve the agent experience and customer interactions. For more information, see Agent training guide.

Released key highlights

Amazon Connect Contact Lens provides the option for you to view key highlights. The highlights show only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript. For more information, see View key highlights.

Released Identity Resolution to consolidate similar profiles

Amazon Connect Customer Profiles offers Identity Resolution, a feature that is designed to automatically detect similar customer profiles by comparing name, email address, phone number, date of birth, and address. For example, two or more profiles with spelling mistakes, such as "John Doe" and "Jhn Doe," can be detected as belonging to the same customer "John Doe" using clustering and matching machine learning (ML) algorithms. Once a group of profiles are detected to be similar, admins can configure how profiles should be merged together by setting up consolidation rules by using the Amazon Connect admin console or Amazon Connect Customer Profiles APIs.

Amazon Connect Customer Profiles stores contact history at no charge

Amazon Connect Customer Profiles now provides contact history and customer information together in unified customer profiles at no charge, helping contact center managers personalize
the contact center experience. In new instances, Customer Profiles is enabled by default. For more information, see Step 4: Data Storage in the Create an Amazon Connect instance topic.

**Added modular flows to help you create common functions**

Flow modules are reusable sections of a flow. You can create them to extract repeatable logic across your flows, and create common functions. For more information, see Flow modules for reusable functions.

**New APIs to archive/unarchive and delete contact flows**

Added new APIs that provide a programmatic and flexible way to manage your library of flows at scale. For example, flows used only during certain times of the year can be archived when not in use and then unarchived when needed. You can now also delete a flow so it is no longer available for use. For more information, see the Amazon Connect API Reference.

**Search contacts by custom contact attributes**

Added support for searching contacts by custom contact attributes (also called user-defined attributes). For more information, see Search by custom contact attributes.

**Added Customer profiles block**

Added the Customer profiles block. It enables you to retrieve, create, and update a customer profile.

**Released Contact APIs**

Added APIs so you can get and update contact details programmatically. For example, you can describe contact details such as queue information, chat attachments, task references, and update contact information such as task name. For more information, see DescribeContact, UpdateContact, and ListReferences in the Amazon Connect API Reference.

**Released scheduled tasks**

Added the ability to schedule tasks up to six days in the future to follow-up on customer issues when promised. You can also update the scheduled date and time using the UpdateContactSchedule API. For more information, see the Create task block and the Create a task topic in the Agent training guide.
Released security profiles APIs

Added APIs so you can create and manage security profiles programmatically. Security profiles help you manage who can access the Amazon Connect dashboard and Contact Control Panel (CCP), and who can perform specific tasks. For more information, see the Amazon Connect API Reference.

Changes to real-time metrics agent tables

We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables are sorted by agent status instead of by agent login.

Additionally, the queues and routing profiles table are sorted by agents online instead of by queue or routing profile name.

Added new metrics

Added following new historical metrics: Contacts transferred in by agent and Contacts transferred out by agent. Added new real-time metrics: Transferred in by agent and Transferred out by agent. For more information, see Historical metrics definitions and Real-time metrics definitions.

October 2021 Updates

Released real-time chat message streaming

You can subscribe to a real-time stream of chat messages. For more information, see Enable real-time chat message streaming.

Released HoursOfWeek APIs for General Availability

Released the Amazon Connect HoursOfWeek APIs for general availability (GA). Also launched AWS CloudFormation support for Users, User Hierarchies, and Hours of Operation. For more information, see the Amazon Connect API Reference and the AWS CloudFormation User Guide.
September 2021 Updates

Released Amazon Connect Wisdom General Availability

Note
In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.

For more information, see Use Amazon Q in Connect for generative AI–powered agent assistance in real-time and the Amazon Q in Connect API Reference.

Amazon Connect Voice ID - General Availability

For more information, see Use real-time caller authentication with Voice ID and the Amazon Connect Voice ID API Reference.

Preview release of Amazon Connect outbound campaigns

Added content for the preview release of outbound campaigns. By using Amazon Pinpoint Journeys and Amazon Connect, you can now create outbound campaigns for voice, SMS, and email. For more information, see Enable outbound campaigns.

New Amazon AppIntegrations Service APIs

New DataIntegration APIs for the Amazon AppIntegrations Service: CreateDataIntegration, DeleteDataIntegration, GetDataIntegration, ListDataIntegrationAssociations, ListDataIntegrations, UpdateDataIntegration.

For more information, see Amazon AppIntegrations Service API Reference.

Display name and contact attributes in chat

You can now personalize the chat experience, as you can specify the name of your customer that interacts using the chat user interface. You can also securely pass the contact attributes to capture information about the contact which can be used in the flow to further personalize the experience. For more information, see Pass the customer display name when a chat initializes and Pass contact attributes when a chat initializes.
Preview of agent application

Launched an updated UI for the agent application preview that combines Customer Profiles and the Contact Control Panel (CCP). For more information, see Access Customer Profiles in the agent application.

Added Create task block

Added the Create task block. It creates a new task, sets the tasks attributes, and initiates a flow to start the task. For more information, see Flow block: Create task.

August 2021 Updates

Improved user interface for Amazon Connect console

Released a redesigned and improved user interface for the Amazon Connect console, making it easier and faster to manage Amazon Connect instances. For more information, see Create an Amazon Connect instance.

APIs for Hours of Operation and Agent Status (Preview)

Released for ungated preview new APIs for managing hours of operation and agent status. For more information, see Amazon Connect Service API Reference.

Contact Lens: Build rules that generate tasks and EventBridge events

Contact Lens rules now allow you to automatically generate tasks and EventBridge events based on uttered keywords, sentiment scores, customer attributes, and other criteria. For more information, see Create rules with Contact Lens.

Networking: Allow AWS Global Accelerator

When using SAML Sign-In to your Amazon Connect instance, you now need to add the AWS Global Accelerator domain, *.awsglobalaccelerator.com, to your allow list. For more information, see Set up your network.

July 2021 Updates

"Next status" feature for the CCP

In busy contact centers, it can be difficult for agents to take a break or go offline when contacts are being quickly routed to them. To help agents manage their time, we have released a feature that
lets agents pause new contacts being routed to them while they finish their current contacts. When all their slots are cleared, Amazon Connect automatically sets agents to the next status, such as Lunch.

For details about how agents use this feature, see Set your "Next status" in the CCP.

**Metrics: No changes due to "Next status"**

When an agent is in **Next status**, their metrics are the same as when their status is **Available**.

For example, an agent is handling one contact and chooses **Next status**. Here’s what you’ll see in the real-time metrics report:

- Agent Activity state = On Contact
- Agent - Staffed = 1

**Non-productive time** (NPT) is not incremented when an agent is in **Next status** because the agent is still **Available**. NPT increments only when the agent actually enters the non-productive status, such as Lunch.

**Agent event stream has new NextAgentStatus field**

When an agent sets their status to **Next status**, Amazon Connect populates a new **NextAgentStatus** field with the next status selected by the agent.

At the same time, the **AgentStatus** field continues to display **Available**.

The following code snippet shows what the agent event stream looks like when an agent has set their CCP to **Next status: Lunch**.

```
"CurrentAgentSnapshot": {
    "AgentStatus": {
        "ARN": "example-ARN",
        "Name": "Available",
        "StartTimestamp": "2019-08-13T20:52:30.704Z"
    },
    "NextAgentStatus": {
        "Name": "Lunch",
        "ARN": "example-ARN2",
    }
}
```
When an agent has not selected a **Next status**, the field is `null`, as shown in the following snippet:

```
"CurrentAgentSnapshot": {
  "AgentStatus": {
    "ARN": "example-ARN",
    "Name": "Available",
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
  },
  "NextAgentStatus": null
}
```

**Amazon Connect Streams API and "Next status"**

The feature has the following effect:

- If you integrate with Amazon Connect Streams API and your agents interact directly with the native CCP user interface, your agents will start using this new feature immediately.

- If you integrate with Amazon Connect Streams API but your agents don't interact directly with the native CCP user interface, your contact center will continue to have the previous behavior when `agent.setState()` is called: an agent will not be able to select an NPT or Offline status while connected to at least one contact.

  If you are handling state change logic yourself from Amazon Connect Streams, you will need to make additional changes explained in the [Amazon Connect Streams README](#).

**Contact search: To search contacts by Agent login requires Users - View permissions in your security profile**

To use the **Agent** filter on the **Contact search** page, in your Amazon Connect security profile you must have **Users - View** permissions, as shown in the following image:
When you have **Users - View** permissions, on the **Contact search** page the **Agent** filter appears, as shown in the following image:

Without **User - View** permissions, the **Agent** filter is not visible, and searching contacts by Agent login is not supported, as shown in the following image:
June 2021 Updates

Apple Messages for Business GA

Released Apple Messages for Business for general availability (GA). For more information, see Enable Apple Messages for Business.

Quick connects management API GA

Released Amazon Connect quick connects management API for general availability (GA). For more information, see Amazon Connect Service API Reference. The quick connects API also supports AWS CloudFormation. For more information, see Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.

Support for Amazon Lex V2 console and APIs

For more information on using the Amazon Lex V2 console with Amazon Connect, see Add an Amazon Lex bot. Added these three APIs: AssociateLexBot, DisassociateLexBot, and ListLexBots. See the Amazon Connect Service API Reference.

Chat: Increase to chat agent concurrency

Chat agents can now handle up to 10 concurrent chat contacts. For more information, see Create a routing profile.
May 2021 Updates

Added contact events

Subscribe to a near real-time stream of contact events (for example, call is queued) in your Amazon Connect contact center. For more information, see Amazon Connect contact events.

Contact search

The following changes were released for Contact search:

- Download increase: You are able to download 3,000 rows of search results to a CSV file, instead of 1,000 rows. This increase applies to contacts that occurred after Dec 01, 2020.
- Contact search supports Disconnect Reason as a new filter on the Contact search page.

The following image shows how Disconnect reason appears in the user interface as a filter.

The following image shows how you can filter by type of disconnect reason. For a definition of each disconnect reason, see the ContactTraceRecord section of the Contact records data model topic.
The following image shows how you add **Disconnect reason** as a column to your search results.

### April 2021 Updates

**Customer Profiles: Identity resolution**

Added identity resolution APIs to Customer Profiles. For more information, see the [GetMatches](#) and [MergeProfiles](#) APIs in the Amazon Connect Customer Profiles API reference.

**Contact Lens: Use category tags to navigate transcript**

For more information, see [Tap or click category tags to navigate through transcript](#).
Fixes for chat metrics

We released fixes for the following issues identified in chat metrics:

• Amazon Connect incorrectly reported that chat contacts that were created from disconnect flows were created from transfer flows.
• When these fixes, Amazon Connect correctly reflects in the contact records and agent event stream that these chat contacts were created from disconnect flows.

There is no impact to voice or task contacts.

Chat contacts created through disconnect flows no longer increment the following metrics:

• Contact flow time
• Contacts incoming
• Contacts handled incoming
• Contacts transferred in

In addition, note the following fixes for contact records and the agent event stream for chat contacts:

• Contact records: There was an issue in the Attributes section of a chat contact record where the initiation method is API for both disconnect and transfer contacts. With this fix, the initiation method correctly reflects Disconnect and Transfer, respectively.
• Agent event stream: Chat contacts created from disconnect flows now have Disconnect as the initiation method.

March 2021 Updates

Amazon Connect is now available in the Canada (Central) Region

Amazon Connect is now available in the Canada (Central) Region. You can claim toll-free and local telephone numbers from Canadian telephony suppliers. For a list of countries were the Canada (Central) Region is supported, see Region requirements for phone numbers. For a list of Contact Lens features available in the Canada (Central) Region, see Availability of Contact Lens features by Region.
Domain for new Amazon Connect instances is "my.connect.aws"

The domain for the Amazon Connect access URL has changed to my.connect.aws.

For example:

- Current: https://[instance name].awsapps.com/connect/
- New: https://[instance name].my.connect.aws/

How does this change impact logging in to Amazon Connect?

The current access URL continues to work for Amazon Connect instances created before the release of the my.connect.aws domain. Any Amazon Connect instances created after the release automatically use the new domain.

Also, if you create new Amazon Connect instances after the release of the new domain, you must add new domains to your allowlist. These domains are in addition to the ones that are currently required.

Currently required domains added to your allow list:

- {myInstanceName}.awsapps.com/connect/ccp-v2
- {myInstanceName}.awsapps.com/connect/api
- *.cloudfront.net

New additional domains to add to your allowlist:

- {myInstanceName}.my.connect.aws/ccp-v2
- {myInstanceName}.my.connect.aws/api
- *.static.connect.aws

For more information, see Set up your network.

Schedule for domain change

The change has been rolled out to all Regions.
March 2021

The following updates were released in March 2021.

When customizing a historical metrics report, you have the option to select a 15 minutes interval, in addition to the current option of a 30 minutes interval.

The 15 minutes interval works the same as the 30 minutes interval. For example, you can query up to three days of data at a time, for the past 35 days.

Chat: Add a chat user interface your website

Added a communications widget that you can customize and secure so it can only be launched from your widget. For more information, see Set up your customer's chat experience.

Provided an open source example. For more information, see Download and customize our open source example.

Amazon Connect Endpoint Test Utility

To help you validate connectivity to Amazon Connect, or troubleshoot when your agents are experiencing problems with the Contact Control Panel (CCP), we've added the Amazon Connect Endpoint Test Utility. For more information, see Use the Endpoint Test Utility.
February 2021 Updates

Contact Lens: Availability of real-time analytics

Content Lens real-time analytics is available in Europe (London), Europe (Frankfurt), and Asia (Tokyo). For more information, see Contact Lens features by Region.

Ingest data into Customer Profiles using Amazon S3

Added the ability to create and ingest data from Amazon S3. For more information, see Create and ingest customer data into Customer Profiles by using Amazon S3.

Disconnect reason in contact record stream

The Amazon Connect contact records stream now includes DisconnectReason for voice calls and tasks. DisconnectReason indicates whether an agent or customer disconnected the call, or whether a telecom or network issue caused a call to disconnect. You can also determine whether a task was completed by an agent or an automatic flow, or it expired. For more information, see ContactTraceRecord.

Custom service levels

Added the ability to create custom service levels. For details, see New metric groupings and categories.

Metrics updates

The following updates were released in February 2021.

New metric groupings and categories

With the release of custom service level metrics, we also made the following changes:

- On the Table settings pages, pre-set and custom service level metrics are in a new group called Contact Service Levels.
- Historical metrics on the Table settings page are grouped into categories.
- The order of metric columns on historical metrics reports changed to match the order of the metrics on the Table settings page.
Following is more information about these changes.

**Real-time metrics: New Contact Service Level category**

A new category of metrics appears on the Table settings page: **Contact Service Level**.

The following image shows this new category on the Table settings page, in an expandable group. Choose the arrow next to the group to view and select the metrics you want to add to your report.

![Table settings screenshot](image)

Use the **Contact Service Level** category to choose pre-set service level metrics, and to create custom service level metrics.

The following image shows the user interface for creating custom service level metrics.
Historical metrics: New categories for metrics

To make it easier to find the historical metrics you want to add to a report, metrics on the Table settings page are grouped into the following categories:

- Agents
- Contacts Abandoned
- Contact Service Level: This group contains preset and custom service levels.
- Contacts Answered
- Performance

Choose Add Custom SL to add custom service levels to your historical metrics report.
The order of the metric columns on the historical metrics reports has changed

The order of the metric columns on the historical metrics reports matches the updated grouping scheme and order of the metrics on the **Table settings** page.

This change supports the addition of custom service level metrics. It also allows us to make future improvements for where, for example, control of how a report looks resides on the **Real-time metrics** page and the **Historical metrics** page, not the **Table settings** page.

Note how metric columns now appear on reports:

- When you open the **Real-time metrics** page, custom service levels appear at the end of the **Performance** group.
- Metrics on existing **Scheduled reports** (the processed documents that arrive in your Amazon S3 buckets) are not re-ordered automatically. However, if you update an existing report, the metrics are re-ordered to match the order on the **Table settings** page.
- **Service level metrics:**
  - Real-time metrics reports: Service level metrics are always added to the end of the **Performance** group, in ascending order.
  - Historical metrics reports: When you add custom service level metrics, they are added to the end of the report in the order they were created.
Custom service level metrics

You have the ability to add custom service level metrics. You can also choose from additional durations, such as minutes, hours, or days.

The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

Group by channel in a historical metrics report

To group by channel on historical metrics reports

1. On the navigation menu, choose Analytics and optimization, Historical metrics, and then choose a report.
2. Choose Settings.
3. On the Table Settings page, choose the Groupings tab. Add Channel, and choose Apply.
4. The table shows a column for **Channel**, as shown in the following image.

**January 2021 Updates**

**CCP: Change your audio settings**

Added the ability to change audio settings from the Contact Control Panel (CCP). This applies to organizations using a customized CCP. For more information, see [How to use the CCP or agent workspace to change your audio device settings](#).

**Queue APIs (Preview)**

Added APIs so you can programatically create and manage queues. For more information, see [Amazon Connect Service API Reference](#).
Amazon AppIntegrations APIs - GA

Released Amazon AppIntegrations APIs for general availability (GA). For more information, see Amazon AppIntegrations Service API Reference.

December 2020 Updates

Quick Connect APIs (Preview)

Added APIs so you can programmatically create and manage quick connects. For more information, see Amazon Connect Service API Reference.

Chat: Support for attachments

Added support for chat attachments. For more information, see Enable attachments to share files using chat and upload files to cases.

Added the following APIs:

- CompleteAttachmentUpload
- GetAttachment
- StartAttachmentUpload

Configurable DTMF timeouts for Lex bots

For more information, see Configurable fields for DTMF input.

Tasks

Added support for tasks, allowing you to prioritize, assign, track, and even automate tasks across the disparate tools agents use to support customers. For more information, see Concepts: Tasks in Amazon Connect.

Amazon Connect APIs

Added an Amazon Connect API that provides the ability to create tasks (StartTaskContact), and a set of preview APIs.

Preview APIs:

- CreateIntegrationAssociation
• DeleteIntegrationAssociation
• ListIntegrationAssociations
• CreateUseCase
• DeleteUseCase
• ListUseCases

Amazon AppIntegrations APIs (Preview)

Added the Amazon AppIntegrations APIs (Preview), which enables you to configure and reuse connections to external applications. For more information, see Amazon AppIntegrations Service API Reference (Preview).

Customer Profiles

Added Amazon Connect Customer Profiles, enabling agents to create a customer profile for every new contact that comes in. You can also integrate with external applications that provide customer profile data. For more information, see Use Customer Profiles and the Amazon Connect Customer Profiles API Reference.

Real-time analytics using Contact Lens

Added real-time analytics for Contact Lens so you can detect and resolve customer issues more proactively while the call is in progress. For more information, see Analyze conversations using conversational analytics and the Amazon Connect Contact Lens API Reference.

Amazon Connect Voice ID (Preview)

Added Amazon Connect Voice ID (Preview), which provides for real-time caller authentication. For more information, see Use real-time caller authentication with Voice ID.

Amazon Connect Wisdom (Preview)

Note

In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.
Added Amazon Connect Wisdom (Preview), which enables agents to search and find content across multiple repositories, such as frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues.

**Amazon Connect with Apple Messages for Business (Preview)**

Added support for using Amazon Connect with Apple Messages for Business. For more information, see [Enable Apple Messages for Business](#).

**November 2020 Updates**

**Telephony call metadata attributes**

- Added call attributes to improve fraud detection and routing. For more information, see [Telephony call metadata attributes (call attributes)](#).

**View historical changes**

- The ability to **View historical changes** on the resource configuration pages is now available for the London Region. The following differences appear as the changes are rolled out to other Regions.
  - Total results: The number feature in the **View historical changes** search page, and page numbers, are replaced with **Previous** and **Next** icons.
  - The Username filter requires the entire login name.

**Chat**

- Added interactive message templates. For more information, see [Add interactive messages to chat](#).

**APIs**

- Added APIs so you can programmatically manage your agent hierarchies and agent groups. For more information, see [Amazon Connect Service API Reference](#).
- Added the following APIs (in an ungated preview release):
  - CreateInstance
• DescribeInstance
• ListInstances
• DeleteInstance
• UpdateInstanceAttribute
• UpdateInstanceStorageConfig

October 2020 Updates

The following updates were released in October 2020:

Flows

• Added chat support for whisper flows. For more information, see Flow block: Set whisper flow.

Metrics

• Released the following real-time metrics:
  • Avg callback connecting time
  • Avg incoming connecting time
  • Avg outbound connecting time

• Released the following historical metrics:
  • Agent API connecting time
  • Agent callback connecting time
  • Agent incoming connecting time
  • Agent outbound connecting time
  • Average agent API connecting time
  • Average agent callback connecting time
  • Average agent incoming connecting time
  • Average agent outbound connecting time

• In real-time metrics reports, added one-click drill-downs. These allow you to drill down into queue and routing profile data in one click. For more information, see Use one-click drill-downs for Routing profiles and Queues tables.
• Added the **Restrict contact access** permission which enables you to manage a user's access to results on the **Contact search** page based on their agent hierarchy group. For more information, see [Search for contacts](#).

• Added **ContactDetails** and **References** to the contact record. For more information, see [Contact records data model](#).

### September 2020 Updates

The following updates were released in September 2020:

#### Service quotas

• Updated the service quotas for the following Amazon Connect Participant Service APIs:
  - [CreateParticipantConnection](#)
  - [DisconnectParticipant](#)
  - [GetTranscript](#)

#### Flows

• Added the Amazon Connect Flow language, a JSON-based representation of a series of flow actions, and the criteria for moving between them. For more information, see [Flow language](#).

#### APIs

Added the following APIs for flows:

- [CreateContactFlow](#)
- [DescribeContactFlow](#)
- [UpdateContactFlowContent](#)
- [UpdateContactFlowName](#)

Added the following API to list prompts:

- [ListPrompts](#)
Added the following APIs for routing profiles:

- `AssociateRoutingProfileQueues`
- `CreateRoutingProfile`
- `DescribeRoutingProfile`
- `DisassociateRoutingProfileQueues`
- `ListRoutingProfileQueues`
- `UpdateRoutingProfileConcurrency`
- `UpdateRoutingProfileName`
- `UpdateRoutingProfileQueues`

### August 2020 Updates

The following updates were released in August 2020:

#### Flows

- Added the ability to automatically use the best sounding voice available from Amazon Polly for text-to-speech. For more information, see [Amazon Polly best sounding voice](#).
- Added the ability to select, cut, copy, and paste flows. For more information, see [Copy and paste flows](#).

#### Telephony

- Added the ability for all customers to enable/disable media support for outbound phone calls. For more information, see [Step 3: Set telephony](#) in the [Create an Amazon Connect instance](#) topic.

#### Monitoring

- Added logging of Amazon Connect Participant Service calls with AWS CloudTrail. For more information, see [Logging Amazon Connect API calls with AWS CloudTrail](#).
Contact Lens for Amazon Connect

- Updated the security profile permissions for the redaction feature. For more information, see [Security profile permissions for Contact Lens](#).

July 2020 Updates

The following updates were released in July 2020:

Flows

- The **Set voice** block supports speaking styles with neural text-to-speech (TTS) voices. For more information, see [Flow block: Set voice](#).

APIs

- Added `StartContactRecording`, `StopContactRecording`, `SuspendContactRecording`, `ResumeContactRecording` to the Amazon Connect Service API.

Contact Lens for Amazon Connect

- Updated Contact Lens for Amazon Connect for general availability. This feature lets you analyze customer-agent conversations, by using speech transcription, natural language processing, and intelligent search capabilities. For more information, see [Analyze conversations using conversational analytics](#).

Metrics

- Fixed content that was added in June 2020 that said **Agent idle time**, **Agent on contact time**, and **Occupancy** had been deprecated. That was incorrect. Rather, they are no longer available for queue groupings only.
- Corrected how **Occupancy** is calculated. The correct calculation is:

  \[
  \text{Occupancy} = \frac{\text{Agent on contact (wall clock time)}}{\text{Agent on contact (wall clock time)} + \text{Agent idle time}}
  \]
June 2020 Updates

The following updates were released in June 2020:

June 2020: Changes for omnichannel support

Group by channel

To group queues or routing profiles by channel on real-time metrics reports

1. On the navigation menu, choose Analytics and optimization, Real-time metrics, and then select either Queues or Routing profiles.

2. Choose Settings.

3. On the Table Settings page, choose the Groupings tab and then select Queues grouped by channels. Or, if you're setting up a Routing profiles report, choose Routing profiles grouped by channels.
4. Choose **Apply**.

5. The table shows a column for **Channel**.

**Group by queue in historical metrics reports**

In the historical metrics report, when you group or filter metrics by **Queue**, the results for the following metrics aren't accurate:

- Agent idle time (not supported in queue grouping as of June, 2020)
- Agent on contact time (not supported in queue grouping as of June, 2020)
- Occupancy (not supported in queue grouping as of June, 2020)

Because of this, on the **Table Settings** page, **Metrics** tab, these metrics are inactive, as shown in the following image:
In addition, in the historical metrics report, Amazon Connect displays a hyphen (-) in place of results for these metrics, and the cells are inactive (gray).

**Effect of queue grouping on saved and scheduled reports**

If the **Queue** grouping or filter is used on the following reports, note these effects:

- **Saved reports.** The columns for these metrics don't appear in the saved reports when grouped by Queue. When the saved report is filtered by Queue, however, it shows "-".
- **Scheduled reports.** These reports continue to run successfully, but no results are returned for these metrics.

**Agent on contact time (not supported in queue grouping as of June, 2020)**

On historical metrics reports when an agent handles multiple chats concurrently, **Agent on contact time** shows wall clock time: the amount of time spent chatting. However, there isn't a metric that shows the time an agent spends chatting with each contact.
In addition, no results are returned when you use the Queue grouping or filter with Agent on contact time.

Agent idle time (not supported in queue grouping as of June, 2020)

The Agent idle time metric divides the idle time into each queue associated with the agent. When contacts are grouped or filtered by Queue, however, Amazon Connect doesn't provide an accurate view into the how the agent is working. Because of this, Amazon Connect doesn't show Agent idle time when you apply the Queue grouping or filter to your report.

Occupancy (not supported in queue grouping as of June, 2020)

With the addition of chat, the Occupancy metric is now defined as the percentage of time that an agent was active on contacts. This percentage is calculated as follows:

\[
\text{Occupancy} = \frac{\text{Agent on contact (wall clock time)}}{\text{Agent on contact (wall clock time)} + \text{Agent idle time}}
\]

Because Agent idle time is now inaccurate when contacts are grouped or filtered by Queues, the Occupancy metric is also inaccurate. As a result, when contacts are grouped or filtered by Queues, Occupancy doesn't appear on the report.

Occupancy no longer appears on the Dashboard page.

Contact Control Panel (CCP)

- Released the following improvements:
  - DTMF input is passed to all lines in a three-way call. Any party can enter DTMF input.
  - Resolved an issue where the DTMF tone degraded when agents interacted with Quick connect and/or Number pad during a session.
  - Resolved an issue where quick connects sometimes did not appear on a page, even after an agent refreshed it.
  - Improved the experience when a manager "listens in" to multiple chat conversations. Updated the unread message count on the CCP to include messages sent by the customer and those sent by the agent. Previously, the unread message count only included messages sent by the customer.
- Published instructions for upgrading to the latest CCP. For more information, see Upgrade to the latest CCP.
• Published a training video that explains how to use the CCP. For more information, see Training video: How to use the CCP.

Flows

• The **Set disconnect flow** block supports voice conversations. For more information, see Flow block: Set disconnect flow.

• The **Set Voice** block supports Amazon Polly Neural Text-to-Speech (NTTS) voices. For more information, see Flow block: Set voice.

• The **Get queue metrics** block can return metrics by channel, for example, by voice or chat. For more information, see Flow block: Get queue metrics.

May 2020 Update

The following updates were released in May 2020:

Flows

• Added the ability to select multiple blocks at the same time and rearrange them as a group within a flow. For more information, see Create an inbound flow.

April 2020 Update

The following updates were released in April 2020:

Telephony

• Added early media support for outbound phone calls. Enabled by default, an agent hears tones and audio messages played by phone companies—such as busy signals, failure to connect errors, or other informational messages—through their headset or audio device. For more information, see Step 3: Set telephony in the Create an Amazon Connect instance topic.

• Added the barge-in-enabled session attribute to the Get customer input block so customers can interrupt Amazon Lex bots with their voice.
March 2020 Update

The following updates were released in March 2020:

**Flows**

- Updated the [Store customer input](#) block to allow you to specify a custom terminating keypress.

**Metrics**

- Announced [June 2020: Changes for omnichannel support](#).

**Networking**

- Updated softphone requirements in [Set up your network](#).

February 2020 Update

The following updates were released in February 2020:

**Service Quotas**

- Adjusted [Amazon Connect service quotas](#) for new accounts.

**Flows**

Updated the following blocks so you can set contact attributes:

- [Set customer queue flow](#)
- [Set hold flow](#)
- [Set whisper flow](#)

January 2020 Update

The following updates were released in January 2020:
Contact Control Panel (CCP)

The following updates were made to the updated Contact Control Panel (ccp-v2):

- Agents can now transfer a contact by double-clicking a quick connect. For more information, see Transfer calls to a quick connect or external phone number.
- The number pad now retains the previously selected country flag so agents don't need to select it every time.
- All strings in the CCP user interface are now localized in available languages.
- Resolved an issue where the color of the call status bar incorrectly displayed as green during a conference call when the call was in the Joined state. It is now blue.
- Resolved an issue where the agent's name was displayed in error messages for missed chats, rather than the customer's name.

Networking

- Updated Set up your network to include requirements for the updated Contact Control Panel (ccp-v2).

December 2019 Update

The following update was released in December 2019:

Monitoring

- Added Contact Lens for Amazon Connect for preview. This feature enables you search conversations for keywords, sentiment scores, and non-talk time. For more information, see Analyze conversations using conversational analytics.
- Added logging of Amazon Connect API calls with AWS CloudTrail. For more information, see Logging Amazon Connect API calls with AWS CloudTrail.

November 2019 Update

The following updates were released in November 2019:
Omnichannel Support

- Added support for chat communications. For more information, see Concepts.

November 2019

Name changes for "Missed" and "Agent status" and "On call"

The following real-time metrics were renamed:

<table>
<thead>
<tr>
<th>Old name</th>
<th>New name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed</td>
<td>Agent non-response</td>
</tr>
<tr>
<td>Agent status</td>
<td>Agent activity</td>
</tr>
<tr>
<td>On call</td>
<td>On contact</td>
</tr>
</tbody>
</table>

For each metric, existing saved reports automatically start displaying the new name; you don't need to do anything for the new name to appear in your reports.

The column order for a saved report containing one of these metrics stays the same. For example, if you previously saved a report where Agent status was the third metric, now when you open that saved report, Agent activity is the name for the third metric.

For Missed, only the name of the metric changed; the underlying calculation stayed the same. We've changing the name of this metric to Agent non-response so it better reflects its definition:

- Agent non-response increments whenever a contact is offered to an agent, and the agent doesn't respond to the contact for whatever reason.

  For example, the agent could have intentionally let the timer run out, or the agent could have forgotten to grant microphone access in the Contact Control Panel and never heard the ring. In these situations, Amazon Connect doesn't drop the contact. Instead, the routing engine will offer it to another available agent, while the customer continues to wait in queue. This means a single contact could result in multiple Agent non-responses before an agent responds and handles the contact.
For **On call**, the name change to **On Contact** applies to the Real-time metrics UI only. You can continue using AGENTS_ON_CALL with the GetCurrentMetricData API to retrieve data for this metric.

**Label updates for "Agent activity" and "Contact state"**

Labels are the values returned in a report. For example, in the following image **Available** and **Basic Routing Profile** are labels.

![Real-time metrics](image)

For **Agent Activity** and **Contact State**, we renamed some of the labels that describe what the agent's current activity is and what's happening with the contact they are currently working on. This way, the labels in the Real-Time Metrics report are more consistent with the labels the agent sees in the Contact Control Panel. They also align with the data returned about these different states in other parts of Amazon Connect.

When the name of **Agent Status** changed to **Agent Activity**, the following labels changed, too:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Before: Agent Status Labels</th>
<th>After: Agent Activity Labels</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent is logged in but offline</td>
<td>Not shown</td>
<td>Not shown</td>
<td></td>
</tr>
<tr>
<td>Agent switches to <strong>Available</strong> in the CCP</td>
<td>Available</td>
<td>Available</td>
<td></td>
</tr>
<tr>
<td>Agent has an incoming call</td>
<td>CallIncoming</td>
<td>Incoming</td>
<td>ContactState = Incoming contact</td>
</tr>
<tr>
<td>Scenario</td>
<td>Before: Agent Status Labels</td>
<td>After: Agent Activity Labels</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Agent has an incoming callback</td>
<td>CallbackIncoming</td>
<td>Incoming</td>
<td>ContactState = Inbound callback</td>
</tr>
<tr>
<td>Agent accepted a callback, which is now making an outbound call to the customer</td>
<td>Calling</td>
<td>On Contact</td>
<td>ContactState = Outbound callback</td>
</tr>
<tr>
<td>Agent makes outbound call (regardless of what status the agent chose in their CCP)</td>
<td>Calling</td>
<td>On Contact</td>
<td>ContactState = Outbound contact</td>
</tr>
<tr>
<td>Agent missed a phone call due to timer expired</td>
<td>MissedCallAgent</td>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td>Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
<tr>
<td>Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
<tr>
<td>After agent hangs up call</td>
<td>After call work</td>
<td>After contact work</td>
<td></td>
</tr>
<tr>
<td>Scenario</td>
<td>Before: Agent Status Labels</td>
<td>After: Agent Activity Labels</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Agent is on Lunch (a custom status)</td>
<td>Lunch</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>Supervisor's activity state if they are monitoring some agent</td>
<td>Monitoring</td>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Agent's activity state if they are connected to customer while being monitored by a supervisor</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
</tbody>
</table>

The following table shows the how the labels changed for **Contact State**.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Label Name Before</th>
<th>Label Name After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent is logged in but offline</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Agent switches to <strong>Available</strong> in the CCP</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Agent has an incoming call</td>
<td>-</td>
<td>Incoming contact</td>
</tr>
<tr>
<td>Agent has an incoming callback</td>
<td>-</td>
<td>Inbound callback</td>
</tr>
<tr>
<td>Agent accepted a callback, which is now making an outbound call to the customer</td>
<td>Initial</td>
<td>Outbound callback</td>
</tr>
<tr>
<td>Scenario</td>
<td>Label Name Before</td>
<td>Label Name After</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Agent makes outbound call (regardless of what status the agent chose in their CCP)</td>
<td>Initial</td>
<td>Outbound contact</td>
</tr>
<tr>
<td>Agent missed a phone call due to timer expired</td>
<td>Missed call</td>
<td>Missed contact</td>
</tr>
<tr>
<td>Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)</td>
<td>Busy</td>
<td>Connected</td>
</tr>
<tr>
<td>Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)</td>
<td>OnHold</td>
<td>On hold</td>
</tr>
<tr>
<td>After agent hangs up call</td>
<td>After call work</td>
<td>After contact work</td>
</tr>
<tr>
<td>Agent is on Lunch (a custom status)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Supervisor's contact state if they are monitoring an agent</td>
<td>Monitoring</td>
<td>Monitoring</td>
</tr>
</tbody>
</table>

### Flows

Added the following flow blocks:

- 
- 

Updated the following flow blocks for chat:

- 
-
User Management

- Added that you can use AWS Identity and Access Management (IAM) with Amazon Connect. For more information, see Identity and access management for Amazon Connect.

Live Media Streaming

- Added that you can capture customer audio for the entire interaction with your contact center. For more information, see Set up live media streaming of customer audio.

API

- Added StartChatContact, ListTagsForResource, TagResource, UntagResource to the Amazon Connect Service API.
- Added the Amazon Connect Participant Service API. These APIs are used chat participants, such as agents and customers.

Contact Control Panel (CCP)

- Updated the CCP so it supports chat. For more information, see Agent training guide for the CCP and agent workspace.

October 2019 Update

The following update was released in October 2019:

Metrics

- The real time metric On call is now incremented whenever an agent is handling a contact who is connected, on hold, in After Contact Work, or the agent is dialog out to a customer.

This metric is available in the Queues tables and Routing Profile tables on the Real time metrics page. It's also returned by the GetCurrentMetricData API as AGENTS_ON_CALL.
June 2019 Update

The following update was released in June 2019:

Flows

• Added flow versioning so you can choose between a saved or published version when you roll back.

May 2019 Updates

The following updates were released in May 2019:

Metrics and Reporting

• Improved the error messages you might encounter when creating, editing, or deleting a scheduled report.
• In the Historical metrics report UI, changed Contacts missed to Agent non-response. This metric appears as Contacts missed in scheduled reports and exported CSV files.
• In the agent event stream, fixed the formatting of the timestamp millisecond so you can better order and analyze the data. To learn more, see Amazon Connect agent event streams.

Contact Control Panel

• Resolved an issue where calling a destroy action (such as connection.destroy) using the Amazon Connect Streams API resulted in different behavior depending on which leg of the conversation it was called from: the agent or the customer. Now calling a destroy action results in the same behavior for both: a busy conversation is moved to After Call Work (ACW) and a conversation in any other state is cleared. If you used the native Contact Control Panel instead of the Amazon Connect Streams API, you weren't impacted by this issue.

April 2019 Updates

The following updates were released in April 2019:

Contact Control Panel

• Resolved an issue where the hold flow didn't run in this case:
• The agent missed a call and then set themselves back to Available.
• Then they were re-routed the same call.
• The agent put that customer on hold while handling the call.

However, taking the customer off hold worked as expected and no other impact occurred.

• Resolved an issue where the Amazon Connect Streams API returned softphoneAutoAccept = FALSE even though Auto-Accept Call was enabled for the agent.

March 2019 Update

The following updates were released in March 2019:

Metrics and Reporting

• Improved the error messages you might encounter when running real-time metrics reports. For example, if you manually configure a real-time metrics report to contain more than 100 queues, we'll display this message: "You've hit the maximum limit of 100 queues. Please reconfigure your report to contain no more than 100 queues." To learn more, see No metrics or too few rows in a queues report?

Contact Control Panel

• Resolved an issue where, in rare cases, an agent already handling an outbound call could have been incorrectly presented with an additional queued callback, even though they are only allowed to handle one contact at a time. Since that agent would have been on contact and not idle, the agent wouldn't have been able to accept the queued callback.

In these cases, the outbound call was not impacted; the agent wouldn't have noticed any differences in the CCP. The callback was presented to another agent instead of being dropped.

February 2019 Updates

The following updates were released in February 2019:

Updates by category

• Contact Routing
• Flows

• Metrics and Reporting

• Contact Control Panel (CCP)

Contact Routing

• Resolved an issue where in rare cases some contacts were not routed to the agent that was available for the longest time.

• Resolved an issue in the user interface where the value displayed for No. of agents staffed for the Basic Routing Profile on the Routing Profiles page was incorrect. The correct number of agents for the routing profile was displayed on the User Management page.

Flows

• Resolved an issue with the flow editor when adding intents in Chrome.

• Resolved an issue where routing priority and age for queued callbacks were not saved.

• Resolved an issue where contact attributes for an outbound whisper flow were not saved.

Metrics and Reporting

• Added EnqueueTimestamp, Duration, and DequeueTimestamp to the contact record for callback contacts.

• Resolved an issue where InitiationTimestamp for callback contacts did not match the time that the callback was created.

• Resolved an issue where users were given an incorrect message when they did not have permissions to edit a report.

Contact Control Panel (CCP)

• Resolved an issue where callbacks were not ringing in the CCP.

January 2019 Updates

The following updates were released in January 2019:
Updates by category

- Contact Routing
- Flows
- Metrics and Reporting

Contact Routing

- Resolved an issue where in rare cases agent transfers were failing.

Flows

- Resolved an issue where agent transfers were failing.
- Resolved an issue that resulted in periodic delays in publishing flow logs.

Metrics and Reporting

- Resolved an issue in real-time metrics reports where the page showed the wrong calculation for Avg queue answer time.
- Resolved an issue where some events were missing from an agent event stream.

December 2018 Updates

The following updates were released in December 2018:

Updates by category

- Metrics and Reporting
- Contact Control Panel (CCP)

Metrics and Reporting

- Resolved an issue where agent event streams were missing agent snapshots during login and logout events.
- Resolved an issue where the contact record detail page displayed timestamps using the timezone selected on the search page.
• Resolved an issue where the AfterContactWork status was overridden.
• Resolved an issue where the timestamps are incorrect if an agent accidentally disconnects while placing a customer on hold.

Contact Control Panel (CCP)
• Resolved an intermittent issue with initialization when an agent configuration is corrupted or null.
• Resolved an issue where pressing Enter to transfer a call did not work.

November 2018 Updates
The following updates were released in November 2018:

Updates by category
• General
• Flows
• Metrics and Reporting

General
• Resolved an issue with auditing.
• Resolved an issue that sometimes resulted in agents being placed in a default state when a contact disconnected when attempting to connect to an agent.
• Resolved an issue that sometimes resulted in newly created agents not being able to log in correctly if the log in attempt occurred immediately after user account was created.

Flows
• Added the new Loop block, which lets you loop through segments of a flow, such as requesting customer information additional times if valid data is not entered.
Metrics and Reporting

- Resolved an issue where callbacks handled were included in the count for incoming contacts in historical reports, but not counted in scheduled reports. Callbacks handled are no longer included in the count for incoming contacts handled in historical reports.
- Improved performance of report generation for reports with a large number of queues and agents in an instance.
- Resolved an issue with how ACW was reported, and backfilled data in customer instances to correct the ACW data for September, October, and November.

October 2018 Updates

The following updates were released in October 2018:

Updates by category

- **General**
- **Metrics and Reporting**
- **API**

General

- Resolved an issue that sometimes resulted in stuck media sessions.

Metrics and Reporting

- Resolved an issue that sometimes resulted in agent names not being displayed correctly in historical reports.
- Resolved an issue that sometimes resulted in the data related to agent Auxiliary states were incorrectly overwritten.

API

- Resolved an issue where the GetCurrentMetrics operation returned the metric OLDEST_CONTACT_AGE in milliseconds instead of seconds.
September 2018 Updates

The following updates were released in September 2018:

Updates by category

• General

• API

General

• Improved page loading times for the User management page.

• Resolved an issue that sometimes caused issues loading the Queues page when there were a large number of quick connects associated with a queue.

API

• Released the UpdateContactAttributes operation for the Amazon Connect API.

August 2018 Updates

The following updates were released in August 2018:

Updates by category

• General

• Contact Routing

• Metrics and Reporting

General

• Added a restriction of 64 characters for the password length for the administrator account created during instance creation.

• Resolved an issue where the Hours of operation page would not load when no days were selected for a saved Hours of operation configuration.
Contact Routing

- Increased the timeout for whispers to 2 minutes for outbound and queued callbacks so that agents have longer to prepare for the incoming call.

Metrics and Reporting

- Modified how the value for the Contacts abandoned metric so that calls that transfer to callbacks are not counted as abandoned contacts.

July 2018 Updates

The following updates were released in July 2018:

Updates by category

- New Features
- General
- Metrics and Reporting
- Flows

New Features

- Outbound caller ID number
- Add an Amazon Lex bot to Amazon Connect
- User Management APIs
- Manage contacts in a queue

General

- Added an error message when attempting to create an admin user during instance creation using "Administrator" as the user name. The user name Administrator is reserved for internal use, and cannot be used to create a user account in Amazon Connect.
- Added support for directory user names that include consecutive dashes.
• Added pagination when displaying security profiles in your instance so that more than 25 security profiles can be displayed.

• Performance optimizations to reduce latency when using the StartOutboundVoiceContact API.

Metrics and Reporting

• Resolved an issue in real-time metrics reports where applied filters were not displayed in the settings page when an additional filter was applied. The settings page now displays the applied filters correctly.

Flows

• Added drop-down menus for contact attributes to make it easier to reference attributes in a flow.

June 2018 Updates

The following updates were released in June 2018:

Updates by category

• General
• Telephony and Voice
• Flows
• Metrics and Reporting
• Contact Control Panel (CCP)

General

• Changed the font in the UI to Amazon Ember for better readability.

Telephony and Voice

• Introduced support for using Amazon Lex bots with Amazon Connect in the US West (Oregon) Region.
• Fixed a bug that in some cases caused a call to drop when a Loop prompt occurred at the same as a call connecting to an agent.

Flows

• Renamed the Set queue block to Set working queue.
• Added a Copy to clipboard button next to the ARN of a flow so you can easily copy the ARN. Choose Show additional flow information under the name of the flow in the designer to display the ARN.
• Added a new Call phone number block, which lets you choose the phone number from your instance to display as the caller ID in an outbound whisper flow. For more information, see Outbound caller ID number.
• Released contact attributes for system metrics, including a new Get metrics block in flows. For more information, see Route based on number of contacts in a queue.

Metrics and Reporting

• Fixed an issue that caused incorrect rendering of the search field in the filters settings for some historical metrics reports.
• Fixed an issue in downloaded reports where the phone number would be blank instead of listing the phone number for calls that were callbacks.
• Login/Logout reports now support 20,000 rows per report generation, up from 10,000.

Contact Control Panel (CCP)

• Added a mute button to the CCP and a mute function to the Streams API so agents can mute and unmute active calls.

April and May 2018 Updates

The following updates were released in April and May 2018:

Updates by category

• General
• Telephony and Voice
• **Flows**

• **Metrics and Reporting**

• **Contact Control Panel (CCP)**

**General**

• New Amazon Polly voices are now automatically made available in Amazon Connect as soon as they are launched. You can use new voices, such as Matthew and Léa, in your flows.

• Updated password enforcement for Amazon Connect user accounts to match requirements for the Amazon Connect admin account created during instance creation.

• Resolved an issue that sometimes resulted in the email addresses not being saved when updating an existing user account.

**Telephony and Voice**

• Service optimizations to reduce latency and improve caller ID for Japanese telephony.

• Customers can now place calls to Jersey and Guernsey in the Channel Islands.

• Added support for keypad numeric input to an Amazon Lex bots when used in an Amazon Connect contact flow. For more information, see [Amazon Connect Now Supports Keypad Input with an Amazon Lex Chatbot](#).

• Reduced latency for the contact control panel, improving the agent user experience.

**Flows**

• Resolved an issue with publishing a flow in the case where an AWS Lambda function block is used in a flow, and the input type for a parameter was changed from Send attribute with a System attribute is changed to Send text. These flows now publish successfully.

• Agent and customer whispers are now maintained with queued callbacks.

• Attributes now correctly persist with queue callbacks.

• Contact attributes are now maintained when using a Loop prompt block in a queue flow.
Metrics and Reporting

- Data for scheduled reports is now delayed by 15 minutes to allow for most recent data to be incorporated in to reports. Previously, in some cases, report data for the final 15 minute period during the scheduled report interval did not get included in scheduled reports. This applies to all report types.

- In metric calculations, the time that an incoming call rings is attributed to idle time if the agent is in idle state before an incoming call.

- The metric **Agent on contact time** now includes time that an agent spent in an auxiliary busy state.

- Published new documentation about metrics.

Contact Control Panel (CCP)

- Added a **Save** button to the settings menu for the CCP when an agent is using a desk phone. The **Save** button saves the deskphone configuration between sessions.

- Agent username is now available as part of agent configuration data in the **Amazon Connect Streams API**.

- Contact attributes are now available when using the streams.js (Streams API) for screenpops after queued callbacks.

- Fixed issue where for some auto-accept calls, the agent continued to hear ringing after accepting and joining the call.

Amazon Connect Document history

The following table describes important changes in each release of the Amazon Connect Administrator Guide. For notification about updates to this documentation, subscribe to the RSS feed.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New metrics: Contacts Answered/Abandoned in X</strong></td>
<td>On the <strong>Real-time metrics</strong> page, you can define custom thresholds for <strong>Contacts abandoned in X</strong> and <strong>Contacts</strong></td>
<td>December 4, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Updated AmazonConnectServiceLinkedRolePolicy</strong></td>
<td>Updated the service-linked role managed policy to use Amazon Pinpoint phone numbers to allow Amazon Connect to send SMS. For a description of the additional actions, see <a href="#">Amazon Connect updates to AWS managed policies</a>.</td>
<td>November 28, 2023</td>
</tr>
<tr>
<td><strong>No-code UI builder for step-by-step guides</strong></td>
<td>This feature allows you to create and manage the UI pages shown to agents in step-by-step guides. Using a drag-and-drop interface you are able to define static and dynamic content for the agent's UI. This includes layouts, styles, and dynamic data, which enables you to control the look and feel of your agent's experience. With this capability, you are able define what gets displayed in your agent's UI during the step-by-step guided experience. For more information, see the <a href="#">No-code UI builder</a> documentation.</td>
<td>November 28, 2023</td>
</tr>
</tbody>
</table>
**Customer Profiles provides a generative AI powered customer data mapping capability**

Customer Profiles provides a generative AI powered customer data mapping capability that significantly reduces the time needed to create unified profiles, which allows you to create more personalized customer experiences more efficiently. For more information, see [Generative AI powered data mapping](#).

**Analytics data lake (Preview)**

You can use Analytics data lake as a central location to query various types of data from Amazon Connect. This data includes contact records and Contact Lens conversational analytics. Data is refreshed around every 24 hours. You can use the Analytics data lake to create custom reports or run SQL queries. For more information, see [Access Analytics data lake](#). For a list of new actions, see the [Analytics data lake actions](#) topic in the *Amazon Connect API Reference*. 

November 28, 2023
Amazon Connect supports two-way SMS

Amazon Connect supports two-way Short Messaging Service (SMS) capabilities, making it easy for you to resolve customer issues by text messaging. SMS offers a ubiquitous and convenient channel for customers to get help, while enabling you to deliver personalized experiences at a lower cost. For more information, see Set up SMS messaging. For a list of new actions, see the Release notes.

November 28, 2023

Amazon Connect provides in-app, web, and video calling

The Amazon Connect in-app, web, and video calling capabilities enable your customers to contact you without ever leaving your web or mobile application. You can use these capabilities to pass contextual information to Amazon Connect. This enables you to personalize the customer experience based on attributes such as the customer's profile or other information, like actions previously taken within the app. For more information, see Set up in-app, web, and video calling capabilities and the StartWebRTCContact action in the Amazon Connect API Reference.

November 28, 2023
Contact Lens provides real-time conversational analytics for chat, extending the machine learning-powered post-contact analytics (for example, sentiment analysis, automated contact categorization, and more) to real-time contact scenarios. For more information, see Analyze conversations using conversational analytics and the ListRealtimeContactAnalysisSegmentsV2 action in the Amazon Connect API Reference.

Contact Lens provides generative AI–powered post-contact summarization, enabling contact center managers to more efficiently monitor and help improve contact quality and agent performance. For more information, see View post-contact summarization powered by generative AI (Preview).
| Added Amazon Q in Connect | Amazon Q in Connect is a generative AI–customer service assistant. It is an LLM-enhanced evolution of Amazon Connect Wisdom that delivers real-time recommendations to help contact center agents resolve customer issues quickly and accurately. For more information, see [Use Amazon Q in Connect for generative AI–powered agent assistance in real-time](#) and the [Amazon Q in Connect API Reference](#). | November 28, 2023 |
| Create quick responses | Quick responses provide pre-written answers to common customer inquiries during a chat conversation. The responses can save time and reduce customer frustration. For more information, see [Create quick responses for use with chat contacts](#) and [Search for quick responses in CCP](#). | November 17, 2023 |
Service Quotas allows you to view both default and applied quota values for resources used by each of your Amazon Connect instances. When requesting a quota increase, Service Quotas allows you to indicate both the Amazon Connect quota and desired value. For quotas that support resource level adjustability you can also specify your Amazon Connect instance. For more information, see Amazon Connect service quotas.

Added an action to AmazonConnectServiceLinkedRolePolicy

Updated AmazonConnectServiceLinkedRolePolicy with an action for Amazon Q in Connect. For a description of the additional action, see Amazon Connect updates to AWS managed policies.

November 16, 2023

November 15, 2023
The prompts configuration user interface has been updated to make it more efficient for you to manage prompts. In addition, when you add, update or delete a prompt from the Amazon Connect admin website, a record of that activity is available in AWS CloudTrail for visibility, reporting, and compliance. For more information about the new prompts page, see Create prompts.

You can integrate Amazon Connect with your preferred file scanning application to detect malware or other unwanted content in attachments before they can be shared in a chat or uploaded to a case. This capability provides an additional layer of protection for your customers and organization by preventing malicious files from being shared and downloaded. For more information, see Set up attachment scanning.
Updated AmazonConnectCampaignsServiceLinkedRolePolicy service-linked role managed policy

November 8, 2023

Updated the service-linked role managed policy for outbound campaigns. For a description of the additional actions, see Amazon Connect updates to AWS managed policies.

Amazon Connect outbound campaigns supports high-volume voice outreach by using the BatchPutContact API. You can use your own list management capability to set up the contact strategy (for example, campaign start and end times, do-not-call times, maximum contact attempts), while programmatically using the Amazon Connect predictive dialer with machine learning (ML)--powered answering machine detection. This increases live-party connections and reduces the amount of time agents waste with unanswered calls. You can also track outcomes of all campaign calls using the Amazon Connect contact record.

November 8, 2023
<table>
<thead>
<tr>
<th>Added new service-linked role policy and service-linked role</th>
<th>You can programmatically add and view author comments by using the <code>CreateRelatedItem</code> and <code>SearchRelatedItems</code> APIs.</th>
<th>November 8, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added AmazonConnectSynchronizationServiceRolePolicy service-linked role policy and AWSServiceRoleForAmazonConnectSynchronization service-linked role for managed synchronization. The policy and role provide access to read, create, update, and delete Amazon Connect resources and is used to automatically synchronize AWS resources across AWS regions. For more information, see <a href="#">AWS managed policy: AmazonConnectSynchronizationServiceLinkedRole Policy</a> and <a href="#">Using service-linked roles for Amazon Connect Managed Synchronization</a>.</td>
<td>November 3, 2023</td>
<td></td>
</tr>
</tbody>
</table>
Added Create persistent chat association flow block and new API

You can set up a chat to be persistent either when the chat session is initially created or at any time during the lifetime of the chat. To set up persistent chat after the chat session has started, use the new `CreatePersistentContactAssociation` API or include the new `Create persistent contact association` block in your flow.
Amazon Connect Global Resiliency customers can use the `ReplicateInstance` API to copy configuration information for resources such as users, routing profiles, queues, and flows across AWS Regions. The API also automatically matches the service quotas for these resources across AWS Regions as part of the replication process. For more information, see [Create a replica of your existing Amazon Connect instance](https://docs.aws.amazon.com/connect/latest/adminguide/tutorials/create-a-replica-instance.html).

Added the `BatchGetFlowAssociation` API. Use this API to obtain a list of flow-associations for the resource identifiers provided in the API request. For example, you can list which phone numbers are associated with which flows in an Amazon Connect instance.
### Added Contact Lens conversational analytics metrics in the API

You can analyze aggregate agent and contact performance using Contact Lens conversational analytics metrics in the `GetMetric DataV2`. The following new metrics were added: non-talk time percent, talk time percent, talk time agent percent, and talk time customer percent. For descriptions of these metrics, see [Historical metrics definitions](#).

**November 2, 2023**

### Added actions to AmazonConnectServiceLinkedRolePolicy

Updated `AmazonConnectServiceLinkedRolePolicy` with actions for Amazon Connect Customer Profiles. For a description of the additional actions, see [Amazon Connect updates to AWS managed policies](#).

**October 30, 2023**

### Increased quota for GetProfileObjectType

Changed default limit for `GetProfileObjectType` from 5 to 10.

**October 28, 2023**
<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party applications preview</td>
<td>You can integrate third-party applications into the agent workspace. For more information, see <a href="https://aws.amazon.com">Third-party applications (3p apps) in the agent workspace (Preview)</a> and the <a href="https://aws.amazon.com">Amazon Connect agent workspace third-party developer guide</a>.</td>
<td>October 27, 2023</td>
</tr>
<tr>
<td>Added actions to AmazonConnectServiceLinkedRolePolicy</td>
<td>Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Wisdom. For a description of the additional actions, see <a href="https://aws.amazon.com">Amazon Connect updates to AWS managed policies</a>.</td>
<td>October 25, 2023</td>
</tr>
<tr>
<td>Updated the definition of Contact handle time</td>
<td>Contact handle time includes the time agents spend in an Offline status making outbound calls.</td>
<td>October 23, 2023</td>
</tr>
<tr>
<td>Added UpdatePhoneNumberMetadata API</td>
<td>Use the UpdatePhoneNumberMetadata to update the metadata for a phone number, such as the phone number description.</td>
<td>October 23, 2023</td>
</tr>
<tr>
<td>Outbound calling restrictions</td>
<td>Added a new topic that explains restrictions that are in place for outbound calling with Amazon Connect: <a href="https://aws.amazon.com">Outbound calling restrictions</a>.</td>
<td>October 16, 2023</td>
</tr>
<tr>
<td>Add as many as four access control tags to a single security profile</td>
<td>Adding additional access control tags will make a given security profile more restrictive. For example, if you add four access control tags like BPO:AcmeCorp, Specialty:Claims, Department:Billing, and City:NewYork, the user would only be able to see resources containing all four of these tags. For more information, see <a href="#">Tag-based access control configuration limitations</a>.</td>
<td>October 16, 2023</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Updated default rate limit for GetContactAttribute and UpdateContactAttribute</td>
<td>For new Amazon Connect instances, the default rate limit for GetContactAttribute and UpdateContactAttribute has been updated. For more information, see <a href="#">API throttling quotas</a>.</td>
<td>October 6, 2023</td>
</tr>
<tr>
<td>Added actions to AmazonConnectServiceLinkedRolePolicy</td>
<td>Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Customer Profiles. For a description of the additional actions, see <a href="#">Amazon Connect updates to AWS managed policies</a>.</td>
<td>October 6, 2023</td>
</tr>
</tbody>
</table>
Create and customize up to 15 communications widgets

You can create and customize up to 15 communications widgets per Amazon Connect instance. For more information, see Add a chat user interface to your website.

October 5, 2023

Access trailing 90 days of historical agent and contact metrics

You can access the trailing 90 days of historical agent and contact metrics (for example, Service level, Average handle time) by using the GetMetricDataV2 API. You can also make requests spanning up to 35 days with data categorized by customizable time intervals such as 15 minutes, hourly, or weekly. Also added five new metrics to the GetMetricDataV2 API. They are not available in the Amazon Connect admin website. For a list, see the Release notes.

October 3, 2023

Amazon Connect Client Application v1.0.2.38 is available

Released Amazon Connect Client Application v1.0.2.38. This version contains minor fixes and improvements. For more information, see Amazon Connect Client Application.

September 29, 2023
| Added actions to AmazonConnectServiceLinkedRolePolicy | Updated AmazonConnectServiceLinkedRolePolicy with actions for Amazon Connect Wisdom. For a description of the additional actions, see Amazon Connect updates to AWS managed policies. | September 29, 2023 |
| Added "View my contacts" permission | Added a new security profile permission: View my contacts. On the Contact search page, agents who have this permission can access the contacts that they've handled. If you're using Contact Lens, agents can also review the analyzed recording and transcripts of the contact. For more information, see Security profile permissions for Contact Lens. | September 25, 2023 |
| Streams API upgrade for third-party cookies | This upgrade prevents the blocking of third-party cookies from impacting Amazon Connect across Chrome and all supported browsers. For more information, see Use Amazon Connect Streams API for third-party cookies. | September 22, 2023 |
Create alerts on real-time metrics

You can create rules that automatically send emails or tasks to managers based on the values of real-time metrics. This enables you to alert managers on contact center operations that could potentially impact the end-customer experience. For more information, see Create alerts on real-time metrics.

September 20, 2023

"Maximum contacts in queue" includes all channels

If you have a queue that combines more than one channel, and you set a custom value for Maximum contacts in queue, the queue stops accepting new contacts after that number is reached, regardless of the distribution of contacts. For example, if you set the value to 50, and the first 50 contacts are chats, then voice calls are not routed to this queue. For more information, see Set the Maximum contacts in queue limit.

September 15, 2023
Manage contacts from the Contact details page

On the **Contact details** page of an in-progress contact, you can manage a contact by transferring, rescheduling, or ending the contact. For more information, see [Manage contacts from the Contact details page](#).

September 14, 2023

Upload file attachments to cases

Agents can upload file attachments to cases. For more information, see [Enable attachments](#). For a list of supported file types, see [Feature specifications](#).

September 11, 2023

Subscribe to the CONTACT_DATA_UPDATED event type in the contact event stream

You can subscribe to an event type called **CONTACT_DATA_UPDATED**. The Contact object includes an UpdatedProperties field. This enables you to monitor for changes to scheduled timestamp for tasks, and changes to user-defined attributes on the contact record. In addition, hierarchy groups information in the AgentInfo object is included for CONTACT_DATA_UPDATED, CONNECTED_TO_AGENT, and DISCONNECTED event types. For more information, see [Contact events data model](#).

September 11, 2023
<table>
<thead>
<tr>
<th><strong>Search for in-progress contacts</strong></th>
<th>You can search for in-progress contacts on the <strong>Contact search</strong> page. For more information, see <strong>Search for in-progress contacts</strong>.</th>
<th>September 11, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APIs to programmatically configure views in step-by-step guides</strong></td>
<td>Amazon Connect provides APIs to programmatically create and manage view resources used in step-by-step guides. View resources define what gets displayed in your agent’s UI during a step-by-step guide. For more information, see the <strong>View resource</strong> documentation.</td>
<td>September 7, 2023</td>
</tr>
<tr>
<td><strong>Support for UIFN in more than 60 countries</strong></td>
<td>Amazon Connect supports Universal International Freephone number (UIFN) in more than 60 countries that are registered with the International Telecommunications Union, an organization that supports the administration of the UIFN service. Amazon Connect allows you to enable UIFNs in as many countries as you need, with a requirement of at least 5 countries. For more information, see <strong>UIFN service</strong>.</td>
<td>September 1, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Voice dialing for outbound campaigns, no agents required</strong></td>
<td>You can use Amazon Connect outbound campaigns for high-volume outreach with no agents required. A new dialer type called &quot;Agentless&quot; makes it easier to proactively communicate with your customers for use cases such as personalized voice notifications and appointment reminders. For more information, see <a href="#">Create an outbound campaign</a> and the <a href="#">CreateCampaign</a> API.</td>
<td>August 31, 2023</td>
</tr>
<tr>
<td><strong>Amazon Connect Cases supports nine additional languages</strong></td>
<td>For more information, see <a href="#">Amazon Connect Cases</a> in the <a href="#">Languages supported by Amazon Connect</a> topic.</td>
<td>August 28, 2023</td>
</tr>
<tr>
<td><strong>Granular access controls using resource tags for the agent activity audit report</strong></td>
<td>You can apply granular permissions to the agent activity audit report in the Amazon Connect historical metrics UI using resource tagging and tag-based access controls. For more information, see <a href="#">tag-based access controls for agent activity audit</a> and <a href="#">tag-based access controls in Amazon Connect</a>.</td>
<td>August 25, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Enhanced user bulk edit</td>
<td>You can now update up to 100 user records on the Amazon Connect admin website in less than half the time it used to take to make bulk updates. This enhancement is especially useful during contact surges when you may need to change the routing profile for many agents. For more information, see <a href="#">Edit users in bulk</a>.</td>
<td>August 24, 2023</td>
</tr>
<tr>
<td>Amazon Connect scheduling supports agent group activities</td>
<td>Amazon Connect scheduling allows contact center managers to more efficiently create and manage activities for groups of agents. For more information, see <a href="#">Add shift activities in draft or published schedules</a>.</td>
<td>August 24, 2023</td>
</tr>
<tr>
<td>GA for global sign-in and agent distribution capabilities</td>
<td>Released the following Amazon Connect Global Resiliency capabilities for general availability: global sign-in and agent distribution across Amazon Connect Regions. For more information, see <a href="#">Set up your agent’s experience with Amazon Connect Global Resiliency</a>. For a list of new APIs associated with this release, see the <a href="#">Release notes for Amazon Connect</a>.</td>
<td>August 10, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Sorting on column header names</td>
<td>You now have the ability to sort by choosing a column header, rather than choosing the smaller arrow next to the header text. For more information about real-time metrics, see <a href="#">Real-time metrics reports</a>.</td>
<td>August 8, 2023</td>
</tr>
<tr>
<td>100 rows on real-time metrics tables</td>
<td>You can now view up to 100 rows in the real-time metrics tables on the Real-time metrics page. Previously, the maximum was 50 rows. For more information about real-time metrics, see <a href="#">Real-time metrics reports</a>.</td>
<td>August 8, 2023</td>
</tr>
<tr>
<td>Route based on time since last inbound contact</td>
<td>Added an option to specify that selected agents with this routing profile will not have their routing order impacted by outbound contacts. For more information, see <a href="#">Create a routing profile</a>.</td>
<td>August 4, 2023</td>
</tr>
<tr>
<td>Use the mini-map to navigate a flow</td>
<td>On the flow designer, the mini-map view to helps you easily navigate the flow. The drag-to-move mini-map has visual highlights that enable you to quickly move to any point in the flow. For more information, see <a href="#">Use the mini-map to navigate a flow</a>.</td>
<td>July 31, 2023</td>
</tr>
</tbody>
</table>
**Undo and redo actions in the flow designer**

For more information, see *Undo and redo actions in the flow designer*.  

**Restrict attributes to specific flows**

Released a new type of attributes called a flow attribute. Flow attributes are restricted to the flow in which they are configured. They are useful in situations where you don't want to persist the data throughout the contact, such as when you need to use sensitive information like the customer's credit card number to do a Lambda data dip. For more information, see *Flow attributes*.  

**Customize the names of flow blocks**

To help you distinguish blocks in a flow, you can customize the names of blocks. For example, you might rename a *Play Prompt* flow block to *Welcome message* or a *Get customer input* flow block to *Hotel booking Lex bot*. For more information, see *Set custom flow block name*.  

July 31, 2023
| Archive, restore, and delete flows and modules | You can archive, restore, and delete flows and modules by using the Amazon Connect admin website. This makes it easier to manage flows and modules that are not in use or no longer needed. For example, flows used only during certain times of the year can be archived when not in use and then unarchived when needed. When a flow has been archived, you can then permanently delete the flow so it is no longer available within your list of flows. For more information, see Archive, restore, and delete flows and modules. | July 31, 2023 |
| Add notes to a block | For more information, see Add notes to a block. | July 31, 2023 |
| Added permissions for using Wisdom page in console | For more information, see Required permissions for using custom IAM policies to manage access to the Amazon Connect console. | July 28, 2023 |
| Streamlined the left nav in the documentation | Streamlined the left navigation menu in the Amazon Connect Administrator Guide to make it easier to navigate. | July 27, 2023 |
Schedule flexible days and shift activities based on shift length

You can generate agent schedules that have the appropriate number of activities, such as breaks or meals, depending on the duration of the shift. The required number of breaks and meals are automatically placed in schedules that are compliant to various regional labor laws. You can generate agent schedules that include flexible days, that is, days that will be optionally scheduled if there's a need. Amazon Connect can automatically generate flexible schedules that are compliant to agent's contracts and regional labor laws, thereby saving time for schedulers. For more information, see Create shift profiles.

July 27, 2023
**Import time off balances**

You can import time off balances for your users. You can also set the group allowance for time off by hour, for each calendar day, for specific time off activities. Amazon Connect uses the time off balance to automatically approve or decline time off requests based on the agent's available net balance and the group allowance for time off. For more information, see [Import an agent's time off balance in a .csv file](#) and [Set group allowance for time off](#).

**Amazon Connect Customer Profiles supports rule-based matching and merging**

Amazon Connect Customer Profiles supports rule-based resolution to match and merge similar profiles into unified ones. This enables you to enhance customer service by granting agents and automated systems access to relevant customer information. As a result, interactions become faster and more personalized for customers. For more information, see [Use Identity Resolution to consolidate similar profiles](#).

July 27, 2023
<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon Connect Client Application v1.0.1.33 is available</strong></td>
<td>Released Amazon Connect Client Application v1.0.1.33. With this newer version you no longer need to restart your desktop after installing the client application. For the download location, see the Amazon Connect Client Application topic.</td>
<td>July 21, 2023</td>
</tr>
<tr>
<td><strong>Amazon Connect Cases provides case assignment</strong></td>
<td>Case assignment helps organizations reduce the time to resolve customer issues by clearly tracking case activities and resolution ownership. Agents can associate a case with a queue or an individual agent for resolution. Agents can view and filter cases assigned to their queue, and managers can directly assign cases to individual agents. For more information, see Set up case assignment.</td>
<td>July 20, 2023</td>
</tr>
<tr>
<td><strong>Updated ordering and porting numbers in Brazil</strong></td>
<td>Process and ID requirements have changed. For more information, see Brazil in the Region requirements for ordering and porting phone numbers topic.</td>
<td>July 19, 2023</td>
</tr>
</tbody>
</table>
You can analyze aggregate agent and contact performance using Contact Lens Conversational Analytics metrics in the GetMetricDataV2 API. The list of metrics include Average contact duration, Average conversation duration, Average greeting time agent, Average holds, Average interruptions agent, Average interruption time agent, Average non-talk time, Average talk time, Average talk time agent, and Average talk time customer. For more information, see Historical metrics definitions and GetMetricDataV2.

Amazon Connect Wisdom delivers ML-powered, real-time recommended information to help chat agents quickly solve customer needs.
| **Delete queues and routing profiles programmatically** | You can delete queues and routing profiles programmatically. For more information, see the following topics in the Amazon Connect API Reference: [DeleteQueue](https://aws.amazon.com/documentation/connect/api-reference/API_DeleteQueue/) and [DeleteRoutingProfile](https://aws.amazon.com/documentation/connect/api-reference/API_DeleteRoutingProfile/). Or see the following CLI topics: `delete-queue` and `delete-routing-profile`. To create an AWS CloudFormation template for queues and routing profiles, see the following topics: [AWS::Connect::Queue](https://aws.amazon.com/documentation/connect/api-reference/API_CreateQueue/) and [AWS::Connect::RoutingProfile](https://aws.amazon.com/documentation/connect/api-reference/API_CreateRoutingProfile/). | July 13, 2023 |
| **Agents can change their audio device settings in the CCP and agent workspace** | You can configure the Contact Control Panel (CCP) or agent workspace to enable agents to select their preferred device for microphone input and audio output, such as voice media and new contact notifications. For more information, see [How to use the CCP to change your audio device settings](https://aws.amazon.com/documentation/connect/api-reference/API_CreateRoutingProfile/). | June 30, 2023 |
New interactive message types

Amazon Connect Chat supports new interactive message types: quick replies and carousels. With quick replies, customers are presented with a list of response options (for example, Yes, No) that they can easily click to reply. Carousels present a set of interactive messages in a horizontally-scrolling format. Your customers can scroll through them and select the best option. For more information, see Add interactive messages to chat.

June 29, 2023

Search for existing tags within an Amazon Connect instance

Amazon Connect provides the ability to search for existing tags within an instance, both programmatically via API and within the UI. When tagging resources, you can search from pre-existing key:value pairs before creating new ones. For more information, see the SearchResourceTags API.

June 27, 2023
<table>
<thead>
<tr>
<th>Added screen recording capabilities</th>
<th>Amazon Connect Contact Lens provides screen recording capabilities, making it easy for you to help agents improve their performance. With screen recording, you can identify areas for agent coaching (for example, long contact handle duration or non-compliance with business processes) by not only listening to customer calls or reviewing chat transcripts, but also watching the agent's actions while they are handling a contact. For more information, see <a href="#">Set up and review agent screen recording</a>.</th>
<th>June 16, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Connect scheduling allows agents to manage time off requests</td>
<td>Amazon Connect scheduling now allows contact center agents to manage their time off requests in a self-serve manner. For more information, see <a href="#">Create time off</a>.</td>
<td>June 15, 2023</td>
</tr>
</tbody>
</table>
Amazon Connect Customer Profiles supports real-time data export of unified customer profiles to an Amazon Kinesis Data Stream. Companies can enable data streaming and automatically receive data for new profiles and updates to existing profiles into their Amazon Kinesis Data Stream. For more information, see [Set up real-time export](#).
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GetMetricDataV2 API: Region availability and new functionality</strong></td>
<td>The GetMetricDataV2 API is available in the AWS GovCloud (US-West) Region. GetMetricDataV2 is now available in all AWS Regions where Amazon Connect is offered. This API enables you to access the trailing 35 days of historical agent and contact metrics (for example, service level, average handle time) with customizable filters and groupings. You can use GetMetricDataV2 to build custom dashboards to measure queue and agent performance over time. For example, you can identify the number of contacts that were disconnected by an agent versus disconnected by a customer hanging up. For more information, see GetMetricDataV2.</td>
<td>June 6, 2023</td>
</tr>
<tr>
<td><strong>Contact Lens theme detection</strong></td>
<td>Contact Lens provides a machine learning powered capability for businesses to help identify top contact drivers by grouping customer conversations into themes. For more information, see Use theme detection to discover issues.</td>
<td>May 24, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Troubleshoot monitoring agent conversations</strong></td>
<td>Added feature specifications for monitoring agent conversations. Added when the multi-party calls and enhanced monitoring feature is and is not enabled on your instance, the number of people who can be on the same agent call at the same time. Added a new topic to help you troubleshoot problems that may occur when supervisors monitor live agent conversations. For more information, see <a href="#">Troubleshoot monitoring agent conversations with Amazon Connect</a>.</td>
<td>May 18, 2023</td>
</tr>
<tr>
<td><strong>New APIs for managing prompts</strong></td>
<td>You can programmatically create and manage prompts using APIs, for example, to extract prompts stored in Amazon Connect and add them to your Amazon S3 bucket. AWS CloudTrail, AWS CloudFormation, and tagging are supported. For more information, see <a href="#">Prompt actions</a> in the <em>Amazon Connect API Reference Guide</em>. Also see <a href="#">AWS::Connect::Prompt</a> in the <em>AWS CloudFormation User Guide</em>.</td>
<td>May 18, 2023</td>
</tr>
<tr>
<td>Added security information for forecasting, capacity planning, and scheduling capabilities</td>
<td>For more information, see <a href="#">Data protection in Amazon Connect</a>.</td>
<td>May 16, 2023</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Updated GetMetricDataV2</td>
<td>GetMetricDataV2 API supports metric data up to the last 35 days. For more information, see <a href="#">GetMetricDataV2</a>.</td>
<td>May 11, 2023</td>
</tr>
<tr>
<td>Rich formatting in chat titles and subtitles</td>
<td>You can add rich formatting to the titles and subtitles of your chat messages. For example, you can add links, italics, bold, numbered lists, and bulleted lists. You use markdown to format your text. For more information, see <a href="#">Rich formatting in titles and subtitles</a> in the <a href="#">Add interactive messages to chat</a> topic.</td>
<td>May 2, 2023</td>
</tr>
<tr>
<td><strong>GA for Amazon Connect evaluation capabilities</strong></td>
<td>Released Amazon Connect evaluation capabilities for general availability. This release includes the capabilities to <a href="#">create rules based on evaluation results</a>, and <a href="#">search for evaluations and evaluation forms</a>. For more information, see <a href="#">Evaluate agent performance</a>. To manage evaluation forms programmatically, see the <a href="#">Evaluation actions</a> in the <em>Amazon Connect API Reference</em>. To create a shared template for evaluation forms, see the <a href="#">AWS::Connect::EvaluationForm resource</a> in the <em>AWS CloudFormation User Guide</em>.</td>
<td>April 25, 2023</td>
</tr>
<tr>
<td><strong>Added new CreateParticipant API</strong></td>
<td>Added the <a href="#">CreateParticipant</a> API which you can use to customize chat flow experiences. You use it to integrate custom participants. For more information, see <a href="#">Customize chat flow experiences by integrating custom participants</a>.</td>
<td>April 21, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Customer Profiles displays case information in the agent workspace</strong></td>
<td>Using Amazon Connect Customer Profiles inside the agent workspace, agents can see cases from third-party case management solutions and Amazon Connect Cases inside a particular customer profile. For more information, see Use Customer Profiles and Access Customer Profiles in the agent workspace.</td>
<td>April 19, 2023</td>
</tr>
<tr>
<td><strong>Updated Set recording and analytics flow block topic</strong></td>
<td>Added information that explains how to disable Contact Lens conversational analytics. See Configuration tips in the Flow block: Set recording and analytics behavior topic.</td>
<td>April 14, 2023</td>
</tr>
<tr>
<td><strong>Updated Service quotas page</strong></td>
<td>Clarified how long it takes for quota increases to be processed. Corrected Scheduled reports per instance to indicate it is not adjustable. For more information, see Amazon Connect service quotas.</td>
<td>April 13, 2023</td>
</tr>
<tr>
<td><strong>Added Wisdom support for Microsoft SharePoint Online</strong></td>
<td>You can choose Microsoft SharePoint Online as knowledge base for Wisdom articles.</td>
<td>April 12, 2023</td>
</tr>
<tr>
<td>Update to Set Voice ID block</td>
<td>Updated the Set Voice ID block so it supports fraud watchlist ID for fraud detection.</td>
<td>April 10, 2023</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Added Cross-channel concurrency</td>
<td>You can configure an agent's routing profile to receive contacts from multiple channels at the same time. For example, while an agent is on a voice contact, they can be offered contacts from any other channels enabled in the routing profile, such as chats and tasks. For more information, see Create a routing profile. Also see the CrossChannelBehavior API.</td>
<td>April 10, 2023</td>
</tr>
<tr>
<td>Search, sort, and filter published agent schedules</td>
<td>Schedulers can quickly search, sort, and filter agent schedules from within the published schedule calendar. For more information, see Search and sort a schedule.</td>
<td>April 4, 2023</td>
</tr>
<tr>
<td>Added staff level shift profile</td>
<td>You can assign a shift profile to individual agents. This is useful to do when, for example, you have part-time agents who are in the same staffing group as your full-time agents, but they require their own shift profile. For more information, see the Associate to shift profile option described in Create staff rules for scheduling.</td>
<td>March 31, 2023</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Updated Set up outbound caller ID</td>
<td>As of March 31, 2023, Amazon Connect no longer sets CNAM configurations. For more information, see CNAM in the Set up outbound caller ID topic.</td>
<td>March 30, 2023</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Create step-by-step guides for your agents</td>
<td>Inside the out-of-the-box Amazon Connect agent workspace, you can create workflows that walk agents through custom UI pages that suggest what to do at a given moment during a customer interaction. You can create guides that help agents identify customer issues and recommend subsequent actions, as well as surface screen-pops and forms for submitting transactions and disposition codes. For more information, see <a href="#">Agent Workspace guided experience</a>.</td>
<td>March 27, 2023</td>
</tr>
<tr>
<td>Added support for nested JSON in Invoke AWS Lambda function flow block</td>
<td>The Invoke AWS Lambda function flow block supports JSON responses. For more information, see <a href="#">Flow block: Invoke AWS Lambda function</a>.</td>
<td>March 27, 2023</td>
</tr>
<tr>
<td>Added support for multiple fraudster watchlists</td>
<td>Every domain has a default watchlist where all existing fraudsters are placed by default. You can create and manage custom watchlists to be evaluated against for known fraudster detection. For more information, see <a href="#">Known fraudster detection</a>, and see new actions in the <a href="#">Amazon Connect Voice ID API Reference</a>.</td>
<td>March 27, 2023</td>
</tr>
<tr>
<td>Added Show View flow block</td>
<td>This block is used to configure UI based workflows that you can surface to users in front end applications. For more information, see Flow block: Show view.</td>
<td>March 27, 2023</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Search and sort schedules in the Schedule Manager</td>
<td>Schedulers can quickly search for schedule names using partial keywords or sort the schedule list based on start date, end date, creation date, or updated date. For more information, see Search and sort a schedule.</td>
<td>March 24, 2023</td>
</tr>
<tr>
<td>Configure multiple IAM roles that can be assigned to a single user when using SAML 2.0</td>
<td>You can configure multiple IAM roles that can be assigned to a single user when using SAML 2.0 which enables you to support user access from multiple identity providers simultaneously. For example, if you are migrating identity providers, you can configure multiple IAM roles associated to a single user and that user will be able to access Amazon Connect from either provider. To learn more about configuring IAM roles for SAML 2.0 in Amazon Connect, see the Configure SAML with IAM for Amazon Connect documentation.</td>
<td>March 17, 2023</td>
</tr>
<tr>
<td>Panel template for interactive chat messages</td>
<td>With a panel template, you can present customers with up to 10 choices under one question in a chat message. For more information, see Add interactive messages to chat.</td>
<td>March 10, 2023</td>
</tr>
<tr>
<td>Added GetMetricDataV2 API</td>
<td>Added the GetMetricDataV2 API to the Amazon Connect API Reference Guide. This API enables you to programmatically access trailing 14 days of historical agent and contact metrics data. It extends the capabilities of the GetMetricData API, provides new historical metrics (for example, the number of contacts disconnected, and the number of callback attempts), and provides the ability to filter metrics with more granularity.</td>
<td>March 8, 2023</td>
</tr>
<tr>
<td>Added permission for managing Amazon Connect Customer Profiles Service Linked Roles</td>
<td>Added iam:CreateServiceLinkedRole which allows you to create service-linked roles for Customer Profiles.</td>
<td>March 7, 2023</td>
</tr>
<tr>
<td>Updated Set up US emergency calling</td>
<td>Updated the steps involved in setting up US emergency calling. For more information, see Set up US emergency calling in Amazon Connect.</td>
<td>March 6, 2023</td>
</tr>
<tr>
<td>Added the DeleteDomain API for Cases</td>
<td>For more information, see the <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html">DeleteDomain API</a> in the Amazon Connect Cases API Reference Guide.</td>
<td>February 24, 2023</td>
</tr>
<tr>
<td>Added new attribute type ENHANCEDCONTACT_MONITORING to Describe, List and Update Instance Attribute APIs</td>
<td>This release updates the APIs: DescribeInstanceAttribute, ListInstanceAttributes, and UpdateInstanceAttribute. You can use it to programmatically enable/disable enhanced contact monitoring using attribute type ENHANCEDCONTACT_MONITORING on the specified Amazon Connect instance. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html#api-monitoring-descrinstanceattribute">DescribeInstanceAttribute</a>, <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html#api-monitoring-listinstanceattributes">ListInstanceAttributes</a>, and <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html#api-monitoring-updateinstanceattribute">UpdateInstanceAttribute</a>.</td>
<td>February 24, 2023</td>
</tr>
<tr>
<td>Added RelatedContactId to StartTaskContact API</td>
<td>You can link together an unlimited number of task contacts using the RelatedContactID parameter supported in the StartTaskContact API. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html#api-monitoring-linkedtasks">Linked tasks</a> and the <a href="https://docs.aws.amazon.com/connect/latest/admin/reference/api-monitoring.html#api-monitoring-starttaskcontact">StartTaskContact API</a> in the Amazon Connect API Reference Guide.</td>
<td>February 24, 2023</td>
</tr>
</tbody>
</table>
### Amazon Connect Cases integrates with AWS PrivateLink

For more information, see [Amazon Connect and interface VPC endpoints (AWS PrivateLink)](https://docs.aws.amazon.com/connect/latest/admin/index.html).

**February 20, 2023**

### Added CONTACT_EVALUATIONS to ResourceType

In the *Amazon Connect API Reference Guide*, added CONTACT_EVALUATION as a valid value to the ResourceType parameter. This affects the following APIs: `AssociateInstanceStorageConfig`, `DescribeInstanceStorageConfig`, `DisassociateInstanceStorageConfig`, `ListInstanceStorageConfig`, and `UpdateInstanceStorageConfig`.

**February 20, 2023**

### Added support to provide visibility into an agent’s next activity

You can view an agent’s next activity in the real-time metrics agent table in the Amazon Connect real-time metrics UI and by using the public API. For more information, see the [NextStatus API reference](https://docs.aws.amazon.com/connect/latest/admin/index.html).

**February 17, 2023**
<table>
<thead>
<tr>
<th><strong>Added support to provide more granular permissions to metrics reports, including new permissions for real-time metrics, historical metrics, and agent activity audit</strong></th>
<th>You can configure more granular permissions to metrics and reports from within security profiles in the Amazon Connect admin website. For more information, see <a href="#">Permissions required to view real-time metrics reports</a> and <a href="#">Agent activity audit permissions</a>.</th>
<th>February 17, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Added support for more granular access controls (using resource tags) to view real-time metrics for agents, queues, and routing profiles</strong></td>
<td>You can enable more granular access controls for real-time metrics by configuring resource tags and access control tags within security profiles in the Amazon Connect admin website. For more information, see <a href="#">Real-time tag-based access control</a> and <a href="#">Tag based access control in Amazon Connect</a>.</td>
<td>February 17, 2023</td>
</tr>
<tr>
<td><strong>S3 Object Lock for the call recordings bucket</strong></td>
<td>You can use Amazon S3 Object Lock in combination with your call recording bucket to help prevent call recordings from being deleted or overwritten for a fixed amount of time, or indefinitely. For more information, see <a href="#">How to set up S3 Object Lock for immutable call recordings</a>.</td>
<td>February 3, 2023</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>CloudFormation templates for instance management</strong></td>
<td>You can use CloudFormation templates to manage Amazon Connect instances for associating Amazon Lex and Lex V2 bots, Lambda functions, security keys, and approved origins—along with the rest of your AWS infrastructure—in a secure, efficient, and repeatable way. For more information, see <a href="https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-type-resource-amazonconnect.html">Amazon Connect resource type reference</a> in the <em>AWS CloudFormation User Guide</em>.</td>
<td>February 2, 2023</td>
</tr>
<tr>
<td><strong>Added information about key highlights</strong></td>
<td>To learn about the agent's key highlights experience in the Contact Control Panel, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/concept-key-highlights.html">Design a flow for key highlights</a>.</td>
<td>January 30, 2023</td>
</tr>
<tr>
<td><strong>Updated Concurrent post-chat analytics jobs quota</strong></td>
<td>Changed <em>Concurrent post-chat analytics jobs</em> quota from 100 to 200. For more information, see <a href="https://aws.amazon.com/contact-lens/quota/">Contact Lens service quotas</a>.</td>
<td>January 27, 2023</td>
</tr>
<tr>
<td>Added persistent chat</td>
<td>Customers often start a chat, then leave the conversation and return later to continue chatting. This may happen many times over the course of several days, months, or even years. To support long running chats like these, you enable persistent chat. For more information, see Enable persistent chat. Also see changes to StartChatContact in the Amazon Connect API Reference Guide, and see the GetTranscript API the Amazon Connect Participant Service API Reference Guide.</td>
<td>January 20, 2023</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Added documentation requirements Brazil, Caribbean, Iceland, and other numbers</td>
<td>Updated documentation requirements for Austria, France, and Japan as well. For more information, see Region requirements for ordering and porting phone numbers.</td>
<td>January 13, 2023</td>
</tr>
<tr>
<td>Added documentation requirements for porting Argentina numbers</td>
<td>For more information, see Region requirements for ordering and porting phone numbers.</td>
<td>January 9, 2023</td>
</tr>
<tr>
<td>Updates to GetCurrentMetricData and GetCurrentUserData</td>
<td>For the <strong>GetCurrentMetricData</strong> API, added support for routing profile filter, sort criteria, and grouping by routing profiles. For the <strong>GetCurrentUserData</strong> API, added support for routing profiles, user hierarchy groups, and agents as filters, and next status and agent status name. For both APIs, added ApproximateTotalCount.</td>
<td>December 23, 2022</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Added message receipts feature for chat messages</strong></td>
<td>The message receipts feature allows customers to receive <em>Message delivered</em> and <em>Read</em> receipts after they send a chat message. For more information, see <a href="#">Enable message Delivered and Read receipts in your chat user interface</a>. Also see the <a href="#">SendEvent</a> action, and the <a href="#">Item, MessageMetadata</a> and <a href="#">Receipt</a> data types in the <em>Amazon Connect Participant Service API Reference Guide</em>.</td>
<td>December 23, 2022</td>
</tr>
<tr>
<td><strong>Microsoft Edge Chromium support</strong></td>
<td>Amazon Connect now supports Microsoft Edge Chromium. For more information about supported browsers, see <a href="#">Browsers supported by Amazon Connect</a>.</td>
<td>December 22, 2022</td>
</tr>
<tr>
<td>Added chat timeouts for chat participants</td>
<td>When a chat conversation between an agent and a customer has been inactive (no messages sent) for a certain amount of time, you may want to consider a chat participant to be idle, and you may even want to automatically disconnect an agent from the chat. To set up chat timeout timers, see Set up chat timeouts for chat participants.</td>
<td>December 22, 2022</td>
</tr>
<tr>
<td>Updated definition of DequeueTimestamp</td>
<td>For the updated definition, see Contact records data model.</td>
<td>December 21, 2022</td>
</tr>
</tbody>
</table>
Amazon Connect supports JSON as a content type for chat messages

By supporting JSON as a content type, Amazon Connect provides you with a way to pass additional information over chat to provide rich personalized experiences. For example, rendering updates to a custom UI, customer-built interactive messages, language translation capabilities, and passing customer metadata to a third party bot. For more information, see **StartChatContact** in the *Amazon Connect API Reference Guide*, and **SendMessage** in the *Amazon Connect Participant Service API Reference Guide*.

**Added feature availability by Region**

Added Amazon Connect features (such as Agent workspace, Tasks, and Wisdom), and the Regions where they are available. For more information, see **Availability of Amazon Connect services by Region**.

**Added topic on Amazon Connect availability by Region**

For more information, see **Availability of Amazon Connect services by Region**.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Lens granular data redaction</strong></td>
<td>When you set up Contact Lens sensitive data redaction, you can choose which entities you want to redact, and how you want the redaction to appear in the transcript. For more information, see Enable redaction of sensitive data.</td>
<td>December 15, 2022</td>
</tr>
<tr>
<td><strong>Released Barge to allow contact center managers to join ongoing calls</strong></td>
<td>Barge allows managers to join and participate in an ongoing customer service call between a contact center agent and customer. After joining the call, a manager can speak with the customer, add participants, and even choose to remove an agent if needed. For more information, see Barge live conversations.</td>
<td>December 14, 2022</td>
</tr>
<tr>
<td><strong>Additional Contact Lens language support and Region availability</strong></td>
<td>Documented that Contact Lens supports the following languages: English - New Zealand, English - South Africa. It is also available in the following Regions: Africa (Cape Town), Asia Pacific (Seoul), Asia Pacific (Singapore).</td>
<td>December 14, 2022</td>
</tr>
<tr>
<td><strong>Added user hierarchy to bulk user upload</strong></td>
<td>You can assign the user hierarchy in the .csv file when you add users in bulk. For more information, see Add users in bulk.</td>
<td>December 13, 2022</td>
</tr>
</tbody>
</table>
### Granular access controls using resource tags for users, security profiles, routing profiles, and queues

You can now enable more granular access controls for security profiles, users, routing profiles, and queues by configuring resource tags within the Amazon Connect console. You can add resource tags to filter and organize these resources logically, and configure access control tags within security profiles to enforce granular permissions. For more information, see [Tagging resources in Amazon Connect](#) and [Tag based access controls in Amazon Connect](#).

**December 9, 2022**

### Bulk user import now includes agent hierarchy and tags

Amazon Connect now allows you to configure hierarchies and resource tags for users in bulk. You can now assign agent hierarchies and resource tags to each agent using the CSV bulk upload template which is available on the user management page. For more information, see [Tagging resources in Amazon Connect](#).

**December 9, 2022**
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules Function language</strong></td>
<td>The Rules Function language is a JSON-based representation of a series of rule conditions. Use it to programmatically add conditions to rules. For more information, see <a href="https://aws.amazon.com/connect/rules-function-language">Amazon Connect Rules Function language</a> in the <em>Amazon Connect API Reference Guide</em>.</td>
<td>December 7, 2022</td>
</tr>
<tr>
<td><strong>Search contacts by agent's first or last name is available in AWS GovCloud</strong></td>
<td>For more information, see <a href="https">Search contacts by agent's first or last name</a>.</td>
<td>December 5, 2022</td>
</tr>
<tr>
<td><strong>GA for Rules APIs</strong></td>
<td>Released a set of Rules APIs that enable you to programmatically create and manage rules. For more information, see <a href="https://aws.amazon.com/connect/rules-actions">Rules actions</a> in the <em>Amazon Connect API Reference</em>.</td>
<td>December 5, 2022</td>
</tr>
<tr>
<td><strong>GA for Forecasting, scheduling, and capacity planning</strong></td>
<td>Released Forecasting, scheduling, and capacity planning for General Availability. These features help you have the right number of agents working at the right times to achieve your operational goals. For more information, see <a href="https://aws.amazon.com/connect/forecasting-capacity-planning-scheduling">Forecasting, capacity planning, and scheduling</a>.</td>
<td>November 29, 2022</td>
</tr>
</tbody>
</table>
Create step-by-step guides for your agents

Inside the out-of-the-box Connect agent workspace, you can now create workflows that walk agents through custom UI pages that suggest what to do at a given moment during a customer interaction. You can create guides that help agents identify customer issues and recommend subsequent actions, as well as surface screen-pops and forms for submitting transactions and disposition codes. For more information, see Agent Workspace guided experience.

Contact Lens supports chat

Amazon Connect Contact Lens provides conversational analytics capabilities for Amazon Connect chat, extending the machine learning powered analytics to better assess chat contacts. For more information, see Analyze conversations using Amazon Connect Contact Lens.
### Added evaluation form features to Contact Lens (Preview)

You can create evaluation forms, and then make them available to managers to review conversations alongside contact details, recordings, transcripts, and summaries, without the need to switch applications. Conversational analytics automatically pre-populates evaluation scores for criteria like script adherence, sensitive data collection, and customer greetings. For more information, see [Evaluate performance (Preview)](#).

**Added configurable Lex timeouts in chat**

You can configure how long to wait for a response from a customer in a chatbot conversation before the session expires. For more information, see *Configurable time-outs for chat input* in the [Get customer input](#) topic.

**Create rules that send email notifications**

You can create Contact Lens rules that send email notifications to people in your organization. For more information, see [Create Contact Lens rules that send email notifications](#).

<table>
<thead>
<tr>
<th>Feature Description</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added evaluation form features to Contact Lens (Preview)</td>
<td>You can create evaluation forms, and then make them available to managers to review conversations alongside contact details, recordings, transcripts, and summaries, without the need to switch applications. Conversational analytics automatically pre-populates evaluation scores for criteria like script adherence, sensitive data collection, and customer greetings. For more information, see <a href="#">Evaluate performance (Preview)</a>.</td>
<td>November 29, 2022</td>
</tr>
<tr>
<td>Added configurable Lex timeouts in chat</td>
<td>You can configure how long to wait for a response from a customer in a chatbot conversation before the session expires. For more information, see <em>Configurable time-outs for chat input</em> in the <a href="#">Get customer input</a> topic.</td>
<td>November 22, 2022</td>
</tr>
<tr>
<td>Create rules that send email notifications</td>
<td>You can create Contact Lens rules that send email notifications to people in your organization. For more information, see <a href="#">Create Contact Lens rules that send email notifications</a>.</td>
<td>November 17, 2022</td>
</tr>
<tr>
<td>Added MonitorContact API</td>
<td>Added a new API for programmatically initiating monitoring of ongoing contacts. For more information, see <a href="#">MonitorContact API</a>.</td>
<td>November 17, 2022</td>
</tr>
<tr>
<td>Search for profiles using multiple search keys</td>
<td>In addition to searching for profiles with a single search key (i.e., a key-values(s) pair), the SearchProfiles API has been enhanced to support searching for profiles using multiple keys and logical operators. This new functionality allows you to use between 1 and 5 search keys with AND or OR logic to find profiles with attributes that match the search criteria. For more information, see the <a href="#">SearchProfiles API reference</a>.</td>
<td>November 14, 2022</td>
</tr>
<tr>
<td>Increased Cases domain quota from 2 to 5</td>
<td>Increased the default maximum number of Cases domains per AWS account from 2 to 5. For more information, see <a href="#">Amazon Connect Cases service quotas</a>.</td>
<td>November 9, 2022</td>
</tr>
<tr>
<td>Added new fields to the GetFederationToken response payload</td>
<td>Added SignInUrl, UserArn, and UserId to the <a href="#">GetFederationToken</a> response payload.</td>
<td>November 9, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Added ability to disable case templates through the UpdateTemplate API</strong></td>
<td>Disabling templates prevents users from creating cases by using the template. For more information, see the <a href="https://docs.aws.amazon.com/connect/latest/api/v2017_07_04/">Amazon Connect Cases API Reference</a>.</td>
<td>November 9, 2022</td>
</tr>
<tr>
<td><strong>Renamed external quick connects to phone number quick connects</strong></td>
<td>For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/overview-quickconnects.html">Types of quick connects</a>.</td>
<td>November 8, 2022</td>
</tr>
<tr>
<td><strong>Delete quick connects using the Amazon Connect console</strong></td>
<td>For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/quickconnect-delete.html">Delete quick connects</a>.</td>
<td>November 4, 2022</td>
</tr>
<tr>
<td><strong>Added DismissUserContact API</strong></td>
<td>Added a new API for programmatically clearing the notifications agents receive after they have missed or rejected a contact, making them eligible to be routed new contacts. This API can also be used to clear similar notifications when an agent encounters an error with accepting the contact or is handling After Contact Work. For more information, see the <a href="https://docs.aws.amazon.com/connect/latest/api/v2017_07_04/#DismissUserContact">DismissUserContact API reference</a>.</td>
<td>November 1, 2022</td>
</tr>
<tr>
<td><strong>Added secondary email address and mobile number to user account</strong></td>
<td>You can now add a secondary email address and mobile number to a user account. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/invite-users.html">Add users to Amazon Connect</a>.</td>
<td>October 28, 2022</td>
</tr>
</tbody>
</table>
Enhanced 911 (E911)  
Enhanced 911 (E911) enables location information to be sent to 911 dispatch when a 911 call is placed. In addition to connecting a user with 911 emergency services, customers in the United States can build E911 capabilities to automatically provide the caller's address information to 911 dispatchers. For more information, see Set up US emergency calling in Amazon Connect.

GA for Amazon Connect Global Resiliency  
Released Amazon Connect Global Resiliency for General Availability. It enables you to provide customer service anywhere in the world with the highest reliability, performance, and efficiency, while meeting international regulatory requirements. For more information, see Set up Amazon Connect Global Resiliency.

Corrected Wisdom service quota  
The originally published quota for Content per knowledge base was incorrect. Corrected the documentation to indicate the quota is 5,000.
<table>
<thead>
<tr>
<th>Feature specifications for the integration association resource</th>
<th>For more information, see Integration association resource feature specifications.</th>
<th>October 13, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added Ctrl+Shift+F to search flow block titles and metadata</td>
<td>For more information, see the Release notes.</td>
<td>October 10, 2022</td>
</tr>
<tr>
<td>GA for Amazon Connect Cases</td>
<td>We've released Amazon Connect Cases for General Availability. Amazon Connect Cases allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see Amazon Connect Cases and Amazon Connect Cases API Reference.</td>
<td>October 3, 2022</td>
</tr>
<tr>
<td>Updated flow designer</td>
<td>We've released a number of improvements to the flow designer experience to make building and editing flows easier. For a detailed list of changes, see Updated flow designer in the Release notes.</td>
<td>September 24, 2022</td>
</tr>
<tr>
<td><strong>Search for Amazon Connect users by first name, last name, and more</strong></td>
<td>You can search for Amazon Connect users by first name, last name, user login, agent hierarchy, security profile, and routing profile. For example, you can search for all Amazon Connect users who have the first name &quot;Jane.&quot;</td>
<td>September 22, 2022</td>
</tr>
<tr>
<td><strong>Visualize historical queue data</strong></td>
<td>You can now visualize historical queue data by using time series graphs to help identify patterns, trends, and outliers specifically for <strong>Service Level</strong>, <strong>Contacts Queued</strong>, and <strong>Average Handle Time</strong>. For more information, see <a href="#">Visualize: Queue dashboard</a>.</td>
<td>September 21, 2022</td>
</tr>
<tr>
<td><strong>Voice spoofing</strong></td>
<td>Use Voice ID to evaluate calls for voice spoofing. For more information, see <a href="#">Voice spoofing detection</a> and the <a href="#">Amazon Connect Voice ID API Reference</a>.</td>
<td>August 29, 2022</td>
</tr>
<tr>
<td><strong>Released SearchSecurityProfiles API</strong></td>
<td>Added a new API for programmatically searching security profiles. For more information, see <a href="#">SearchSecurityProfiles</a>.</td>
<td>August 19, 2022</td>
</tr>
<tr>
<td><strong>Released Schedule Adherence (Preview)</strong></td>
<td>Contact center supervisors or managers track schedule adherence to understand when agents are following the schedule that you have created. This helps ensure you achieve your service level targets, while improving agent productivity and customer satisfaction. For more information, see <a href="https://aws.amazon.com">Schedule Adherence</a>.</td>
<td>August 1, 2022</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Attachments per chat conversation now at 35</strong></td>
<td>Updated the limit for attachments per chat conversations from 5 to 35. See <a href="https://aws.amazon.com">Feature specifications</a>.</td>
<td>July 20, 2022</td>
</tr>
<tr>
<td><strong>Added Voice ID Flow language actions</strong></td>
<td>Added topics for the following Voice ID Flow language actions: <a href="https://aws.amazon.com">CheckOutboundCallStatus</a>, <a href="https://aws.amazon.com">CheckVoiceId</a>, and <a href="https://aws.amazon.com">StartVoiceIdStream</a>.</td>
<td>July 19, 2022</td>
</tr>
<tr>
<td><strong>Search for contacts by using the agent's first or last name</strong></td>
<td>You can search for contacts using the agent's first or last name. The filter name is <a href="https://aws.amazon.com">Agent</a>.</td>
<td>July 15, 2022</td>
</tr>
<tr>
<td>Released updates for rich text format rendering</td>
<td>On the <strong>Contact Search</strong> and <strong>Contact Detail</strong> pages, you can now view chat transcripts that have rich text formatting, such as bold or italic font, bullet points, numbered lists, and hyperlinks. For more information about getting started with Amazon Connect Chat, see <a href="#">Set up your customer's chat experience</a>.</td>
<td>July 13, 2022</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>View call transcript in CCP or agent application</td>
<td>For more information, see <a href="#">View a call transcript during ACW</a>.</td>
<td>July 7, 2022</td>
</tr>
<tr>
<td>Added feature specifications for Contact Lens</td>
<td>For more information, see <a href="#">Amazon Connect Contact Lens feature specifications</a>.</td>
<td>July 1, 2022</td>
</tr>
<tr>
<td>Support for Lex intent confidence scores and sentiment analysis</td>
<td>You can further personalize the automated self-service customer experience using Amazon Lex intent confidence scores and sentiment analysis as a branch within your flows. For more information, see the <a href="#">Get customer input</a> block. For a list of new contact attributes see <a href="#">Amazon Lex contact attributes</a>.</td>
<td>June 29, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>GA for Amazon Connect Outbound Campaigns</strong></td>
<td>Released Amazon Connect Outbound Campaigns, formally known as High-volume outbound communications, for General Availability. This release includes a set of APIs for creating and managing outbound campaigns. For more information, see <a href="https://docs.aws.amazon.com/AmazonConnect/latest/adminguide/enable-outbound-campaigns.html">Enable Amazon Connect outbound campaigns</a> and <a href="https://docs.aws.amazon.com/AmazonConnect/latest/adminguide/">Amazon Connect Amazon Connect Outbound Campaigns API Reference</a>.</td>
<td>June 20, 2022</td>
</tr>
<tr>
<td><strong>Amazon Connect Cases (Preview)</strong></td>
<td>Amazon Connect Cases (Preview) allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see <a href="https://docs.aws.amazon.com/AmazonConnect/latest/adminguide/amazon-connect-cases-preview.html">Amazon Connect Cases (Preview)</a> and <a href="https://docs.aws.amazon.com/AmazonConnect/latest/adminguide/amazon-connect-cases-api-reference-preview.html">Amazon Connect Cases API Reference (Preview)</a>.</td>
<td>June 20, 2022</td>
</tr>
<tr>
<td><strong>Updated Amazon Lex bot per instance quota</strong></td>
<td>Updated the Amazon Lex bot per instance quota from 50 to 70. For more information, see <a href="https://docs.aws.amazon.com/AmazonConnect/latest/adminguide/amazon-connect-service-quota.html">Amazon Connect service quotas</a>.</td>
<td>June 7, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>New GetCurrentUserData API</td>
<td>Released the <a href="#">GetCurrentUserData</a> API. It enables you to return the real-time active user data from the specified Amazon Connect instance.</td>
<td>June 6, 2022</td>
</tr>
<tr>
<td>Released task templates</td>
<td>You can now create custom task templates, making it easy for agents to consistently capture the relevant and required information to create or complete tasks. For more information, see <a href="#">Create task templates</a>. For information about using the API to programmatically create and manage task templates, see the <a href="#">Amazon Connect API Reference</a> and the <a href="#">Amazon Connect Resource Type Reference</a> in the <a href="#">AWS CloudFormation User Guide</a>.</td>
<td>June 2, 2022</td>
</tr>
<tr>
<td>New API to transfer contacts</td>
<td>Added a new API that you can use to transfer contacts from one agent or queue to another agent or queue at any point after a contact is created. For information, see <a href="#">TransferContact</a> in the <a href="#">Amazon Connect API Reference</a>.</td>
<td>June 2, 2022</td>
</tr>
<tr>
<td>Updated workflow for outbound campaigns</td>
<td>Updated the workflow for onboarding to outbound campaigns using the Amazon Connect and Amazon Pinpoint user interface. For more information, see <a href="#">Enable outbound campaigns</a>.</td>
<td>May 27, 2022</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Voice ID expires speakers</td>
<td>For BIPA Compliance, Amazon Connect Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years. You can see a speaker's last access time by looking at the <code>lastAccessedAt</code> attribute returned by the <code>DescribeSpeaker</code> and <code>ListSpeakers</code> APIs, and the <a href="#">What data is stored?</a> section of the Amazon Connect Admin Guide.</td>
<td>May 25, 2022</td>
</tr>
<tr>
<td>Search Voice ID results</td>
<td>Added topic <a href="#">Search and review Voice ID results</a>.</td>
<td>April 28, 2022</td>
</tr>
<tr>
<td>New API to change agent's current status</td>
<td>Amazon Connect provides an API to programmatically change the current status of an agent. <strong>Agent statuses</strong> are used to determine when an agent is <strong>Available</strong> to be routed contacts in Amazon Connect, versus when they are set to <strong>Offline</strong> or a custom status such as <strong>Lunch</strong> or <strong>Break</strong> and should not be routed contacts. For more information, see <a href="#">PutUserStatus</a> in the <a href="#">Amazon Connect API Reference</a>.</td>
<td>April 28, 2022</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>New APIs</strong></td>
<td>Added API to search for user records by first name, last name, username, routing profile, security profile, agent hierarchies or tags. Added API to claim new phone numbers and configure them programmatically. For more information, see the <a href="#">Amazon Connect API Reference</a>.</td>
<td>April 25, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Multi-party calls</strong></td>
<td>You can enable Amazon Connect to allow up to six parties on a call: the agent, the caller, and four more participants. For more information, including a comparison of how multi-party calling differs from the default three-party calling, see <a href="#">Telephony: Multi-party calls</a>.</td>
<td>April 6, 2022</td>
</tr>
<tr>
<td><strong>Play prompts from an Amazon S3 bucket</strong></td>
<td>Added the ability to source prompts from an Amazon S3 bucket. This enables you to store as many voice prompts as needed in Amazon S3 and access them in real time using contact attributes in the following flow blocks that play prompts: Get customer input, Loop prompts, Play prompt, and Store customer input.</td>
<td>April 5, 2022</td>
</tr>
<tr>
<td><strong>Real-time contact analysis segment streams</strong></td>
<td>Added support for accessing Contact Lens analytics in near real-time. For more information, see <a href="#">Use streaming for real-time contact analysis</a>.</td>
<td>March 28, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Rich messaging for chat</td>
<td>Added support for rich messaging for your customer’s chat experience. Agents and customers can use bold, italic, bulleted lists, numbered list, hyperlinks, and attachments. For more information, see <a href="#">Enable text formatting for your customer's chat experience</a>.</td>
<td>March 13, 2022</td>
</tr>
<tr>
<td>Object type mapping user interface</td>
<td>Added a user interface for creating object type mapping by using the Amazon Connect admin console. For more information, see <a href="#">Create an object type mapping</a>.</td>
<td>March 8, 2022</td>
</tr>
<tr>
<td>Updates to AmazonConnectServiceLinkedRolePolicy</td>
<td>Added actions for Amazon CloudWatch metrics. For more information, see <a href="#">Amazon Connect updates to AWS managed policies</a>.</td>
<td>February 22, 2022</td>
</tr>
<tr>
<td>Added bulk ingestion of data for Customer Profiles</td>
<td>For more information, see <a href="#">Bulk ingestion of data</a> in the <a href="#">Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk</a> topic.</td>
<td>February 21, 2022</td>
</tr>
<tr>
<td>New quotas for APIs</td>
<td>For <a href="#">StartChatContact</a>, <a href="#">StartContactStreaming</a>, <a href="#">StopContactStreaming</a>, a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second.</td>
<td>February 11, 2022</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>New CloudWatch metrics for chat</strong></td>
<td>Added the following Amazon CloudWatch metrics for chat: <code>ConcurrentActiveChats</code>, <code>ConcurrentActiveChatsPercentage</code>, <code>ChatBreachingActiveChatQuota</code>, and <code>SuccessfulChatsPerInterval</code>. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/monitoring-instance-cloudwatch.html">Monitoring your instance using CloudWatch</a>.</td>
<td>February 11, 2022</td>
</tr>
<tr>
<td><strong>Documented Rules feature specifications</strong></td>
<td>Documented the feature specifications for Amazon Connect Rules. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/amazon-connect-rules.html">Amazon Connect Rules feature specifications</a>.</td>
<td>January 28, 2022</td>
</tr>
<tr>
<td><strong>Documented Identity Resolution quotas</strong></td>
<td>Documented three quotas for Identity Resolution. For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/amazon-connect-identity-resolution.html">Customer Profiles quotas</a>.</td>
<td>January 28, 2022</td>
</tr>
<tr>
<td><strong>Configure maximum chat duration</strong></td>
<td>You can configure the total duration per chat to be up to 7 days, including wait time. For more information, see the <code>ChatDurationInMinutes</code> parameter in the <a href="https://docs.aws.amazon.com/connect/latest/userguide/api-request-start-chat-contact.html">StartChatContact API</a>.</td>
<td>January 27, 2022</td>
</tr>
<tr>
<td><strong>Contact Lens supports custom vocabularies</strong></td>
<td>For more information, see <a href="https://docs.aws.amazon.com/contact-lens/latest/userguide/add-custom-vocabularies.html">Add custom vocabularies</a>.</td>
<td>January 25, 2022</td>
</tr>
<tr>
<td><strong>Released tagging support for UserHierarchyGroup resource</strong></td>
<td>For more information, see <a href="https://docs.aws.amazon.com/connect/latest/userguide/amazon-connect-user-hierarchy-group-resource.html">CreateUserHierarchyGroup</a>.</td>
<td>January 20, 2022</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Communications widget supports browser notifications</strong></td>
<td>For more information, see <a href="#">Browser notifications</a>.</td>
<td>December 21, 2021</td>
</tr>
<tr>
<td><strong>Integrate Customer Profiles with Segment and Shopify</strong></td>
<td>For more information, see <a href="#">Set up integration for Segment</a> and <a href="#">Set up integration for Shopify</a>.</td>
<td>December 20, 2021</td>
</tr>
<tr>
<td><strong>Updated compliance for tasks</strong></td>
<td>Tasks is in compliance with GDPR, and is approved for SOC, PIC, HITRUST, ISO, and HIPAA.</td>
<td>December 17, 2021</td>
</tr>
<tr>
<td><strong>Released unified agent application</strong></td>
<td>Amazon Connect released the unified agent application to improve the agent experience and customer interactions. For more information, see <a href="#">Agent training guide</a>.</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td><strong>Released key highlights</strong></td>
<td>Amazon Connect Contact Lens provides the option for you to view key highlights. The key highlights show only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript. For more information, see <a href="#">View key highlights</a>.</td>
<td>November 30, 2021</td>
</tr>
<tr>
<td><strong>Documented Average API Connecting Time</strong></td>
<td>Documented the real-time metric <a href="#">Average API Connecting Time</a>. For more information, see <a href="#">Average API Connecting Time</a>.</td>
<td>November 26, 2021</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Released Identity Resolution to consolidate similar profiles</strong></td>
<td>Amazon Connect Customer Profiles offers Identity Resolution, a feature that is designed to automatically detect similar customer profiles by comparing name, email address, phone number, date of birth, and address. For more information, see <a href="#">Use Identity Resolution to consolidate similar profiles</a> and the <a href="#">Amazon Connect Customer Profiles API Reference</a>.</td>
<td>November 24, 2021</td>
</tr>
<tr>
<td><strong>Updated Customer Profiles service quotas</strong></td>
<td>Amazon Connect Customer Profiles now supports 1000 objects per profile (increased from 100), and 50MB Maximum size of all objects for a profile (increased from 5MB). For more information, see <a href="#">Amazon Connect Customer Profiles service quotas</a>.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>Change Description</td>
<td>Details</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Amazon Connect Customer Profiles stores contact history at no charge</td>
<td>Amazon Connect Customer Profiles now provides contact history and customer information together in unified customer profiles at no charge, helping contact center managers personalize the contact center experience. In new instances, Customer Profiles is enabled by default. For more information, see Step 4: Data Storage in the Create an Amazon Connect instance topic.</td>
<td>November 23, 2021</td>
</tr>
<tr>
<td>New APIs to archive/unarchive and delete flows</td>
<td>Added new APIs that provide a programmatic and flexible way to manage your library of flows at scale. For example, flows used only during certain times of the year can be archived when not in use and then unarchived when needed. You can now also delete a flow so it is no longer available for use. For more information, see the Amazon Connect API Reference.</td>
<td>November 22, 2021</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Added modular flows to help you create common functions</strong></td>
<td>Flow modules are reusable sections of a flow. You can create them to extract repeatable logic across your flows, and create common functions. For more information, see <a href="#">Flow modules for reusable functions</a>.</td>
<td>November 22, 2021</td>
</tr>
<tr>
<td><strong>Search contacts by custom contact attributes</strong></td>
<td>Added support for searching contacts by custom contact attributes (also called user-defined attributes). For more information, see <a href="#">Search by custom contact attributes</a>.</td>
<td>November 15, 2021</td>
</tr>
<tr>
<td><strong>Added Customer profiles block</strong></td>
<td>Added the <a href="#">Customer profiles block</a>. It enables you to retrieve, create, and update a customer profile.</td>
<td>November 15, 2021</td>
</tr>
<tr>
<td><strong>Updated AmazonConnect_FullAccess</strong></td>
<td>Added permissions for managing Amazon Connect Customer Profiles. See <a href="#">Amazon Connect updates to AWS managed policies</a>.</td>
<td>November 12, 2021</td>
</tr>
<tr>
<td><strong>Released security profiles APIs</strong></td>
<td>Added APIs so you can create and manage security profiles programmatically. For more information, see the <a href="#">Amazon Connect API Reference</a>.</td>
<td>November 12, 2021</td>
</tr>
</tbody>
</table>
**Released scheduled tasks**

Added the ability to schedule tasks up to six days in the future to follow-up on customer issues when promised. You can also update the scheduled date and time using the `UpdateContactSchedule` API. For more information, see the [Create task](https://docs.aws.amazon.com/connect/latest/adminguide/task-block.html) block and the [Create a task](https://docs.aws.amazon.com/connect/latest/adminguide/task-topic.html) topic in the *Agent training guide*.  

**November 12, 2021**

---

**Released Contact APIs**

Added APIs so you can get and update contact details programmatically. For example, you can describe contact details such as queue information, chat attachments, task references, and update contact information such as task name. For more information, see [DescribeContact](https://docs.aws.amazon.com/connect/latest/adminguide/api-reference.html#connect-api-summary), [UpdateContact](https://docs.aws.amazon.com/connect/latest/adminguide/api-reference.html#connect-api-summary), and [ListReferences](https://docs.aws.amazon.com/connect/latest/adminguide/api-reference.html#connect-api-summary) in the *Amazon Connect API Reference*.  

**November 12, 2021**
Changes to real-time metrics
agent tables

We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables are sorted by agent status instead of by agent login. Additionally, the queues and routing profiles table are sorted by agents online instead of by queue or routing profile name.

November 12, 2021

Added actions to AmazonConnectServiceLinkedRolePolicy

Added actions for Amazon Connect Customer Profiles. See Amazon Connect updates to AWS managed policies.

November 12, 2021

Added new metrics

Added following new historical metrics: Contacts transferred in by agent and Contacts transferred out by agent. Added new real-time metrics: Transferred in by agent and Transferred out by agent. See Historical metrics definitions and Real-time metrics definitions.

November 9, 2021

Released real-time chat message streaming

You can subscribe to a real-time stream of chat messages. For more information, see Enable real-time chat message streaming.

October 29, 2021
<table>
<thead>
<tr>
<th><strong>Cross-service confused deputy prevention for Customer Profiles</strong></th>
<th>Updated <strong>Cross-service confused deputy prevention</strong> with more sample policies you can apply for Amazon Connect Customer Profiles.</th>
<th>October 26, 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GA for HoursOfOperation APIs</strong></td>
<td>Released the Amazon Connect HoursOfOperation APIs for general availability (GA). Also launched AWS CloudFormation support for Users, User Hierarchies, and Hours of Operation. For more information, see the <a href="#">Amazon Connect API Reference</a> and the <a href="#">AWS CloudFormation User Guide</a>.</td>
<td>October 22, 2021</td>
</tr>
<tr>
<td><strong>Example: Programmatically integrate S3 with Customer Profiles</strong></td>
<td>Added a topic that shows how to <a href="#">programmatically integrate S3 with Customer Profiles</a>.</td>
<td>October 21, 2021</td>
</tr>
<tr>
<td><strong>Cross-service confused deputy prevention</strong></td>
<td>Added a topic with example policies you can apply for <strong>Cross-service confused deputy prevention</strong>.</td>
<td>October 18, 2021</td>
</tr>
<tr>
<td><strong>How long unanswered callbacks stay in queue</strong></td>
<td>In the <a href="#">Set up queued callback</a> topic, clarified that unanswered queued callbacks stay in queue at least 7 days and up to 14 days before Amazon Connect automatically removes them.</td>
<td>October 13, 2021</td>
</tr>
<tr>
<td>Updated endpoint for client-side metrics</td>
<td>In the <a href="#">Set up your network</a> topic, changed the endpoint for client-side metrics from <code>*.execute-api.{region}.amazonaws.com</code> to <code>*.telemetry.connect.{region}.amazonaws.com</code></td>
<td>October 11, 2021</td>
</tr>
<tr>
<td>Corrected errors in Service quota topic</td>
<td>Corrected errors in the <a href="#">Service quotas</a> topic: For Amazon Connect Wisdom, <strong>Maximum size per document</strong> is 1MB not 10MB. For Amazon Connect Customer Profiles, the name of the quota is <strong>Object Types per domain</strong> not <strong>Objects per domain</strong>. Updated the Amazon Connect Voice ID quotas table with correct information.</td>
<td>October 8, 2021</td>
</tr>
<tr>
<td>Preview release of outbound campaigns</td>
<td>Added content for the preview release of outbound campaigns. By using Amazon Pinpoint Journeys and Amazon Connect, you can now create outbound campaigns for voice, SMS, and email. For more information, see <a href="#">Enable outbound campaigns</a>.</td>
<td>September 27, 2021</td>
</tr>
</tbody>
</table>
### New Amazon AppIntegrations Service APIs

New DataIntegration APIs for the Amazon AppIntegrations Service: CreateDataIntegration, DeleteDataIntegration, GetDataIntegration, ListDataIntegrationAssociations, ListDataIntegrations, UpdateDataIntegration. For more information, see [Amazon AppIntegrations Service API Reference](#).

September 27, 2021

<table>
<thead>
<tr>
<th>Amazon Connect Wisdom - General Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.</td>
</tr>
</tbody>
</table>

September 27, 2021

<table>
<thead>
<tr>
<th>Amazon Connect Voice ID - General Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>For more information, see <a href="#">Use real-time caller authentication with Voice ID</a> and the <a href="#">Amazon Connect Voice ID API Reference</a>.</td>
</tr>
</tbody>
</table>

September 27, 2021
| Added new service-linked role policy | Added AmazonConnectVoiceIDFullAccess. Use this AWS managed policy so you can set up your users to use Voice ID. This policy provides full access to Amazon Connect Voice ID through the AWS console, SDK, or other means. For more information, see AWS managed policy: AmazonConnectVoiceIDFullAccess. | September 27, 2021 |
| Added new service-linked role policy | Added AmazonConnectCampaignsServiceLinkedRolePolicy, a new service-linked role policy for outbound campaigns. The policy provides access to retrieve all the outbound campaigns. For more information, see Enable outbound campaigns. | September 27, 2021 |
Display name and contact attributes in chat

You can now personalize the chat experience, as you can specify the name of your customer that interacts using the chat user interface. You can also securely pass the contact attributes to capture information about the contact which can be used in the flow to further personalize the experience. For more information, see Pass the customer display name when a chat initializes and Pass contact attributes when a chat initializes.

Preview of agent application

Launched an updated UI for the agent application preview that combines Customer Profiles and the Contact Control Panel (CCP). For more information, see Access Customer Profiles in the agent application.

Added Create task block

Added the Create task block. It creates a new task, sets the tasks attributes, and initiates a flow to start the task. For more information, see Flow block: Create task.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>More languages for Contact Lens</strong></td>
<td>Contact Lens now supports the following languages for post-call and real-time analytics: Japanese, Korean, and Mandarin. The following languages are supported for real-time analytics: French (Canada), French (France), Portuguese (Brazil), German (Germany), and Italian (Italy). For more information, see Contact Lens for Amazon Connect in the Languages supported by Amazon Connect topic.</td>
<td>September 13, 2021</td>
</tr>
<tr>
<td><strong>Updated historical metrics definitions</strong></td>
<td>Updated the definitions of Contacts transferred in and Contacts transferred out. For more information, see Historical metrics definitions.</td>
<td>September 10, 2021</td>
</tr>
<tr>
<td><strong>Improved user interface for Amazon Connect console</strong></td>
<td>Released a redesigned user interface for the Amazon Connect console, making it easier and faster to manage Amazon Connect instances. For more information, see Create an Amazon Connect instance.</td>
<td>August 27, 2021</td>
</tr>
<tr>
<td><strong>Customer Profiles is HIPAA compliant</strong></td>
<td>Customer Profiles is now HIPAA compliant. Removed note stating it is not.</td>
<td>August 23, 2021</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Porting numbers in Singapore</td>
<td>Updated documentation requirements. For more information, see <a href="#">Singapore</a> in the <em>Region requirements for ordering and porting phone numbers</em> topic.</td>
<td>August 10, 2021</td>
</tr>
<tr>
<td>APIs for hours of operation and agent status</td>
<td>Released for ungated preview new APIs for managing hours of operation and agent status. For more information, see <a href="#">Amazon Connect Service API Reference</a>.</td>
<td>August 6, 2021</td>
</tr>
<tr>
<td>Contact Lens rules create tasks and EventBridge events</td>
<td>Contact Lens rules now allow you to generate tasks and EventBridge events based on uttered keywords, sentiment scores, customer attributes, and other criteria. For more information, see <a href="#">Build rule with Contact Lens</a>.</td>
<td>August 5, 2021</td>
</tr>
<tr>
<td>Countries you can call by default</td>
<td>We have updated the list of countries you can call by default when you create a new instance in a given Region. For more information, see <a href="#">Countries you can call</a>.</td>
<td>August 4, 2021</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Add AWS Global Accelerator to your allowlist</td>
<td>When using SAML Sign-In to your Amazon Connect instance, you now need to add the AWS Global Accelerator domain, *.awsglobalaccelerator.com, to your allowlist. For more information, see <a href="#">Set up your network</a>.</td>
<td>August 3, 2021</td>
</tr>
<tr>
<td>New &quot;Next status&quot; feature</td>
<td>To help agents manage their time, we have released a feature that lets agents pause new contacts being routed to them while they finish their current contacts. For more information, see &quot;Next status&quot; feature for the CCP.</td>
<td>July 30, 2021</td>
</tr>
<tr>
<td>Update to Contact search functionality</td>
<td>To use the Agent filter on the Contact search page, in your Amazon Connect security profile you must have Users - View permissions. For more information, see <a href="#">Contact search: To search contacts by Agent login requires Users - View permissions in your security profile</a>.</td>
<td>July 23, 2021</td>
</tr>
<tr>
<td>Added two task metrics sent to CloudWatch</td>
<td>Amazon Connect sends the following two new metrics to CloudWatch: ConcurrentTasks and ConcurrentTasksPercentage. For more information, see <a href="#">Monitoring your instance using CloudWatch</a>.</td>
<td>July 7, 2021</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Updated required permissions for custom IAM policies</td>
<td>Added permissions for Amazon Lex. For more information, see Amazon Connect updates to AWS managed policies.</td>
<td>June 29, 2021</td>
</tr>
<tr>
<td>Apple Messages for Business GA</td>
<td>Released Apple Messages for Business for general availability (GA). For more information, see Enable Apple Messages for Business.</td>
<td>June 28, 2021</td>
</tr>
<tr>
<td>Quick connects management API GA</td>
<td>Released Amazon Connect quick connects management API for general availability (GA). For more information, see Amazon Connect Service API Reference. The quick connects API also supports AWS CloudFormation. For more information, see Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.</td>
<td>June 24, 2021</td>
</tr>
<tr>
<td>Added service quota for Amazon Lex V2 bot aliases per instance = 100</td>
<td>For more information about service quotas, see Amazon Connect service quotas.</td>
<td>June 17, 2021</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Support for Amazon Lex V2 console and APIs</strong></td>
<td>For information on using the Amazon Lex V2 console, see <a href="#">Add an Amazon Lex bot</a>. Added these three APIs: AssociateLexBot, DisassociateLexBot, and ListLexBots. See the <a href="#">Amazon Connect Service API Reference</a>.</td>
<td>June 15, 2021</td>
</tr>
<tr>
<td><strong>Coming soon: Faster load times for Real-time metrics page</strong></td>
<td>Rollout to all Regions July 19, 2021, to September 19, 2021, subject to change. For more information, see <a href="#">Upcoming change: Faster reload times for the Real-time metrics page</a>.</td>
<td>June 11, 2021</td>
</tr>
<tr>
<td><strong>Coming soon: New DataIntegration APIs</strong></td>
<td>On May 20, 2021, we published that new DataIntegration APIs were added to the Amazon AppIntegrations service. These APIs are not yet available.</td>
<td>June 8, 2021</td>
</tr>
<tr>
<td><strong>Chat agent concurrency increased</strong></td>
<td>Increased chat agent concurrency from 5 to 10. For more information, see <a href="#">Create a routing profile</a>.</td>
<td>June 7, 2021</td>
</tr>
<tr>
<td><strong>Object type mapping for Customer Profiles</strong></td>
<td>Added object type mapping for the Customer Profiles standard profile. For more information, see the <a href="#">Object type mapping for the standard profile</a>.</td>
<td>June 1, 2021</td>
</tr>
<tr>
<td>Channels supported by blocks</td>
<td>Added a topic that lists all the blocks and which channels each one supports. For more information, see the <a href="#">Channels each block supports</a>.</td>
<td>May 18, 2021</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Added contact events</td>
<td>For more information, see the <a href="#">Amazon Connect contact events</a>.</td>
<td>May 12, 2021</td>
</tr>
<tr>
<td>Announced upcoming change to Agent audit report</td>
<td>In a future release, you'll be able to download the Agent audit report. For more information, see the <a href="#">Upcoming changes: Download the Agent audit report</a>.</td>
<td>May 4, 2021</td>
</tr>
<tr>
<td>Added identity resolution APIs (preview) to Customer Profiles</td>
<td>For more information, see the <a href="#">GetMatches</a> and <a href="#">MergeProfiles</a> APIs in the Amazon Connect Customer Profiles API reference.</td>
<td>April 30, 2021</td>
</tr>
<tr>
<td>Added topic on how to apply permissions that restrict which AWS resources can be associated with Amazon Connect</td>
<td>For more information, see the <a href="#">Restrict AWS resources that can be associated with Amazon Connect</a>.</td>
<td>April 28, 2021</td>
</tr>
<tr>
<td>Added chapter on architectural guidance, authored by AWS Solution Architects</td>
<td>For more information, see the <a href="#">Architectural guidance for Amazon Connect</a>.</td>
<td>April 28, 2021</td>
</tr>
<tr>
<td>Announced upcoming fix to agent event stream</td>
<td>For more information, see the <a href="#">Upcoming change: Fix for agent event stream</a>.</td>
<td>April 27, 2021</td>
</tr>
<tr>
<td>Change Date</td>
<td>Change Description</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------</td>
<td></td>
</tr>
<tr>
<td>April 24, 2021</td>
<td>Revised the topics on porting phone numbers. For more information, see Port your phone number.</td>
<td></td>
</tr>
<tr>
<td>April 22, 2021</td>
<td>Using Customer Profiles with CCP out-of-the-box is in ungated preview. For more information, see Access the Customer Profiles Agent UI.</td>
<td></td>
</tr>
<tr>
<td>April 20, 2021</td>
<td>Announced upcoming changes for Contact search. For more information, see Upcoming changes: Contact search.</td>
<td></td>
</tr>
<tr>
<td>April 15, 2021</td>
<td>Added NLB endpoint for Canada (Central) Region. Updated Set up your network with the NLB endpoint for Canada (Central) Region.</td>
<td></td>
</tr>
<tr>
<td>March 31, 2021</td>
<td>Amazon Connect is now available in the Canada (Central) Region. You can claim toll-free and local telephone numbers from Canadian telephony suppliers. For a list of countries that support the Canada (Central) Region, see Region requirements for phone numbers. Also see Availability of Contact Lens features by Region.</td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Announced upcoming fixes for chat metrics</strong></td>
<td>Currently Amazon Connect incorrectly reports that chat contacts that were created from disconnect flows were created from transfer flows. When the fixes are released, Amazon Connect will correctly reflect in the contact records and agent event stream that these chat contacts were created from disconnect flows. For more information, see <a href="#">Upcoming change: Fixes for chat metrics</a> in the Release notes.</td>
<td>March 25, 2021</td>
</tr>
<tr>
<td><strong>Completed release of new domain name</strong></td>
<td>The domain for the Amazon Connect access URL has changed to <code>my.connect.aws</code>. For more information, see <a href="#">March 2021 Updates</a> in the Release notes.</td>
<td>March 22, 2021</td>
</tr>
<tr>
<td><strong>Default service quota for reports per instance</strong></td>
<td>Updated the default service quota for reports per instance to 2000. This default applies to accounts created in October, 2020 or later. For more information, see <a href="#">Amazon Connect service quotas</a>.</td>
<td>March 16, 2021</td>
</tr>
<tr>
<td><strong>Identification requirements for ordering and porting phone numbers</strong></td>
<td>Added identification requirements for ordering phone numbers. Added requirements for ordering and porting phone numbers from Argentina, Chile, Mexico, Peru, and Puerto Rico. For more information, see Region requirements for phone numbers.</td>
<td>March 11, 2021</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Use the Amazon Connect Endpoint Test Utility</strong></td>
<td>To help you validate connectivity to Amazon Connect, or troubleshoot when your agents are experiencing problems with the Contact Control Panel (CCP), we added the Amazon Connect Endpoint Test Utility. For more information, see Use the Endpoint Test Utility.</td>
<td>March 5, 2021</td>
</tr>
<tr>
<td><strong>Add a chat user interface to your website.</strong></td>
<td>Added a communications widget that you can customize and add to your website. Also provided an open source example to help you get started with adding chat to your website. For more information, see Set up your customer’s chat experience.</td>
<td>March 5, 2021</td>
</tr>
<tr>
<td><strong>Content Lens real-time analytics is available in Europe (London), Europe (Frankfurt), and Asia (Tokyo).</strong></td>
<td>For more information, see Availability of Contact Lens features by Region.</td>
<td>February 26, 2021</td>
</tr>
<tr>
<td>Added ability to create and ingest data into Customer Profiles from Amazon S3</td>
<td>For more information, see <a href="#">Create and ingest data into Customer Profiles from Amazon S3</a>.</td>
<td>February 25, 2021</td>
</tr>
<tr>
<td>Added DisconnectReason to the contact record stream</td>
<td>The Amazon Connect contact records stream now includes <strong>DisconnectReason</strong> for voice calls and tasks. For more information, see <a href="#">ContactTraceRecord</a>.</td>
<td>February 19, 2021</td>
</tr>
<tr>
<td>Added custom service levels</td>
<td>Added the ability to create custom service levels, and update the metrics user interface. For details, see <a href="#">New metric groups and categories</a>.</td>
<td>February 16, 2021</td>
</tr>
<tr>
<td>Queue APIs (Preview)</td>
<td>Added APIs so you can programmatically create and manage queues. <a href="#">Queue APIs (Preview)</a>.</td>
<td>January 29, 2021</td>
</tr>
<tr>
<td>Amazon AppIntegrations APIs - GA</td>
<td>Released Amazon AppIntegrations APIs for general availability (GA). For more information, see <a href="#">Amazon AppIntegrations APIs - GA</a>.</td>
<td>January 29, 2021</td>
</tr>
<tr>
<td>New Contact search page</td>
<td>Updated the <strong>Contact search</strong> page. For more information, see <a href="#">Search for contacts</a>.</td>
<td>January 5, 2021</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Amazon Connect Service API Reference</td>
<td>Added APIs so you can programmatically create and manage quick connects. For more information, see Amazon Connect Service API Reference.</td>
<td>December 22, 2020</td>
</tr>
<tr>
<td>Chat: Support for sharing attachments</td>
<td>Added support for sharing chat attachments. For more information, see Chat: Support for attachments.</td>
<td>December 21, 2020</td>
</tr>
<tr>
<td>Configurable DTMF timeouts for Lex bots</td>
<td>Added support for configurable DTMF timeouts for Lex bots. For more information, see Configurable DTMF timeouts for Lex bots.</td>
<td>December 4, 2020</td>
</tr>
<tr>
<td>Amazon Connect with Apple Messages for Business (Preview)</td>
<td>Added support for using Amazon Connect with Apple Messages for Business. For more information, see Amazon Connect with Apple Messages for Business (Preview)</td>
<td>December 3, 2020</td>
</tr>
<tr>
<td>Tasks</td>
<td>Added support for tasks, allowing you to prioritize, assign, track, and even automate tasks across the disparate tools agents use to support customers. For more information, see Tasks.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Real-time analytics using Contact Lens for Amazon Connect</strong></td>
<td>Added real-time analytics for Contact Lens so you can detect and resolve customer issues more proactively while the call is in progress. For more information, see <a href="#">Analyze Conversations with Contact Lens for Amazon Connect</a>.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td><strong>Amazon Connect Wisdom (Preview)</strong></td>
<td>In November 2023 we released Amazon Q. It includes real-time agent assist functionality formerly known as Amazon Connect Wisdom, along with generative AI-powered recommended responses, actions, and links to more information.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td><strong>Amazon Connect Voice ID (Preview)</strong></td>
<td>Added Amazon Connect Voice ID (Preview), which provides for real-time caller authentication. For more information, see <a href="#">Amazon Connect Voice ID (Preview)</a>.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td><strong>Amazon Connect Customer Profiles</strong></td>
<td>Added Amazon Connect Customer Profiles, enabling agents to create a customer profile for every new contact that comes in. You can also integrate with external applications that provide customer profile data. For more information, see <a href="#">Amazon Connect APIs</a>.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Amazon Connect APIs</strong></td>
<td>Added an Amazon Connect API that provides the ability to create tasks (<strong>StartTask Contact</strong>) and added a set of preview APIs. For more information, see <a href="#">Amazon Connect APIs</a>.</td>
<td>December 1, 2020</td>
</tr>
<tr>
<td><strong>Amazon Connect supports interact messages for chat</strong></td>
<td>Added interactive message templates. For more information, see <a href="#">Add interactive messages to chat</a>.</td>
<td>November 24, 2020</td>
</tr>
<tr>
<td><strong>Telephony call metadata attributes</strong></td>
<td>Added call attributes to improve fraud detection and routing. For more information, see <a href="#">Telephony call metadata attributes (call attributes)</a>.</td>
<td>November 20, 2020</td>
</tr>
<tr>
<td><strong>APIs to manage user hierarchies</strong></td>
<td>Added APIs so you can programmatically manage your agent hierarchies and agent groups. For more information, see <a href="#">Amazon Connect Service API Reference</a>.</td>
<td>November 18, 2020</td>
</tr>
<tr>
<td><strong>Service quotas</strong></td>
<td>Noted that up to 700 quick connects can be added to a queue. See <a href="#">Feature specifications</a>. (This update was published erroneously and has since been removed.)</td>
<td>October 5, 2020</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Security</td>
<td>Added new topic on <a href="#">Required permissions for managing access to the Amazon Connect console.</a></td>
<td>September 24, 2020</td>
</tr>
<tr>
<td>Quick filters</td>
<td>Added new topic that explains how to use quick filters in real-time metrics reports. For more information, see <a href="#">Use quick filters to drill into Routing profiles and Queues tables.</a></td>
<td>September 23, 2020</td>
</tr>
<tr>
<td>Service quotas</td>
<td>Updated the service quotas for the following Amazon Connect Participant Service APIs: CreateParticipantConnection, DisconnectParticipant, and GetTranscript. For more information, see <a href="#">Amazon Connect Participant Service API throttling quotas.</a></td>
<td>September 22, 2020</td>
</tr>
<tr>
<td>Show agent queues in a Queues table.</td>
<td>By default, agent queues don't appear in a Queues table in a historical metrics report. You can choose to show them. For more information, see <a href="#">Show agent queues in a Queues table.</a></td>
<td>September 18, 2020</td>
</tr>
<tr>
<td>Migrate contact flows to a different instance</td>
<td>You can migrate hundreds of flows using a set of flow APIs. For more information, see <a href="#">Migrate contact flows to a different instance.</a></td>
<td>September 18, 2020</td>
</tr>
</tbody>
</table>

脚注: [Required permissions for managing access to the Amazon Connect console.](#)
Languages supported by Amazon Connect
Learn about which languages are supported in the Amazon Connect console, Contact Control Panel, Contact Lens, Amazon Lex, and Amazon Polly. For more information, see Languages supported by Amazon Connect.

Amazon Connect Flow language
You can use the Amazon Connect Flow language to efficiently update flows that you're migrating from one instance to another, and Write flows rather than drag blocks onto the flow designer. For more information, see Amazon Connect Flow language in the Amazon Connect API Reference Guide.

Option 2 (not recommended): Allow IP address ranges
Removed tip from Option 2: Allow IP address ranges, that said if you don't see an entry for your region, use GLOBAL. For more information, see Option 2 (not recommended): Allow IP address ranges.
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist

Updated Option 1, second row of table, with a line break between {myInstanceName}.awsapps.com/connect/api and *.cloudfront.net. For more information, see Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.

Updated Option 1, second row of table, with a line break between {myInstanceName}.awsapps.com/connect/api and *.cloudfront.net. For more information, see Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allowlist.

September 11, 2020

Amazon Connect resource-level policy examples

Changed title of "Amazon Connect resource-based policy examples" topic to "Amazon Connect resource-level policy examples." For more information, see Amazon Connect resource-level policy examples.

September 8, 2020

Earlier updates

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated the Consult and Contact consulted metrics to indicate they were deprecated May 2019.</td>
<td>For more information, see Consult and Contacts consulted.</td>
<td>August 27, 2020</td>
</tr>
<tr>
<td>Added topic on setting up agent-to-agent transfers.</td>
<td>For more information, see Set up agent-to-agent transfers.</td>
<td>August 19, 2020</td>
</tr>
<tr>
<td>Added section on requirements for custom termination points.</td>
<td>For more information, see Request numbers, international numbers, or termination points.</td>
<td>August 18, 2020</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Removed the &quot;Known differences&quot; section from I use the Amazon Connect Streams API.</td>
<td>For more information, see I use the Amazon Connect Streams API.</td>
<td>August 3, 2020</td>
</tr>
<tr>
<td>Changed the name of the Metrics chapter to Monitor metrics &amp; run reports.</td>
<td>For more information, see Real-time and historical metrics dashboards and reports.</td>
<td>July 16, 2020</td>
</tr>
<tr>
<td>Clarified that the following metrics are no longer supported in queue grouping: Agent on contact time, Agent idle time, Occupancy. Previously we stated that these metrics had been deprecated.</td>
<td>For more information, see June 2020: Changes for omnichannel support.</td>
<td>July 8, 2020</td>
</tr>
<tr>
<td>Updated the Set disconnect flow block, which now supports voice conversations.</td>
<td>For more information, see Set disconnect flow.</td>
<td>June 29, 2020</td>
</tr>
<tr>
<td>Added upcoming metric changes: new real-time and historical metrics for inbound and outbound contact time</td>
<td>For more information, see Real-time and historical metrics dashboards and reports.</td>
<td>June 26, 2020</td>
</tr>
<tr>
<td>Added how to upgrade CCP</td>
<td>For more information, see Upgrade to the latest CCP.</td>
<td>June 16, 2020</td>
</tr>
<tr>
<td>Added video on using CCP</td>
<td>For more information, see Training video: How to use the CCP.</td>
<td>June 16, 2020</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Deprecated metrics: Agent on contact time, Agent idle time, Occupancy.</td>
<td>For more information, see <a href="#">June 2020: Changes for omnichannel support</a>.</td>
<td>June 12, 2020</td>
</tr>
<tr>
<td>Added topic on quick connects work</td>
<td>For more information, see <a href="#">How quick connects work</a>.</td>
<td>May 21, 2020</td>
</tr>
<tr>
<td>Added how to get administrative support, and added a topic on inherited permissions</td>
<td>For more information, see <a href="#">Get administrative support for Amazon Connect</a> and <a href="#">About inherited permissions</a>.</td>
<td>April 16, 2020</td>
</tr>
<tr>
<td>Added how to customize your CCP to log out agents automatically when they close the CCP window</td>
<td>For more information, see <a href="#">CCPv1: Log out agents automatically when they close their CCP</a>.</td>
<td>April 16, 2020</td>
</tr>
<tr>
<td>Updated the <strong>Get customer input</strong> block to support timeout values for voice input</td>
<td>For more information, see <a href="#">Get customer input</a>.</td>
<td>April 8, 2020</td>
</tr>
<tr>
<td>Added terminating keypress</td>
<td>For more information, see <a href="#">Store customer input</a>.</td>
<td>March 31, 2020</td>
</tr>
<tr>
<td>Added NLB endpoints and required domain for softphones</td>
<td>For more information, see <a href="#">Set up your network</a>.</td>
<td>March 23, 2020</td>
</tr>
<tr>
<td>Announced upcoming changes for metrics</td>
<td>For more information, see <a href="#">June 2020: Changes for omnichannel support</a>.</td>
<td>March 23, 2020</td>
</tr>
<tr>
<td>Added topic on region requirements for phone numbers</td>
<td>For more information, see <a href="#">Region requirements for ordering and porting phone numbers</a>.</td>
<td>March 11, 2020</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Added tutorials</td>
<td>For more information, see Tutorials: An introduction to Amazon Connect.</td>
<td>March 6, 2020</td>
</tr>
<tr>
<td>Added topic on emergency admin access</td>
<td>For more information, see Emergency admin login.</td>
<td>March 3, 2020</td>
</tr>
<tr>
<td>Added topics on saving, sharing, and publishing reports</td>
<td>For more information, see Save custom reports, Share custom reports, View a shared report, and Publish reports.</td>
<td>January 22, 2020</td>
</tr>
<tr>
<td>Updated flow block definitions</td>
<td>For more information, see .</td>
<td>January 17, 2020</td>
</tr>
<tr>
<td>Added a section about queued callbacks in metrics reporting.</td>
<td>For more information, see About queued callbacks in metrics.</td>
<td>January 17, 2020</td>
</tr>
<tr>
<td>Updated networking guidance for the updated CCP (ccp-v2)</td>
<td>For more information, see Set up your network.</td>
<td>January 15, 2020</td>
</tr>
<tr>
<td>Add a topic on logging Amazon Connect API calls with AWS CloudTrail</td>
<td>For more information, see Logging Amazon Connect API calls with AWS CloudTrail.</td>
<td>December 13, 2019</td>
</tr>
<tr>
<td>Added a section on analyzing conversations</td>
<td>For more information, see Analyze conversations using conversational analytics.</td>
<td>December 02, 2019</td>
</tr>
<tr>
<td>Added information about live media streaming</td>
<td>For more information, see Set up live media streaming of customer audio.</td>
<td>November 21, 2019</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Added information about chat</td>
<td>For more information, see <a href="http://example.com">Web and mobile messaging.</a> Also added these topics: <a href="http://example.com">Best practices for Amazon Connect</a>, <a href="http://example.com">About agent status</a>, <a href="http://example.com">About contact states</a>, and <a href="http://example.com">Additional resources for Amazon Connect.</a></td>
<td>November 21, 2019</td>
</tr>
<tr>
<td>Added topic on using IAM</td>
<td>For more information, see <a href="http://example.com">Identity and access management for Amazon Connect.</a></td>
<td>November 14, 2019</td>
</tr>
<tr>
<td>Added dimensions</td>
<td>Added dimensions to the Amazon Connect metrics sent to CloudWatch. See <a href="http://example.com">Monitoring your instance using CloudWatch.</a></td>
<td>October 22, 2019</td>
</tr>
<tr>
<td>Added a networking topic</td>
<td>Consolidated networking content into <a href="http://example.com">Set up your network.</a> Updated the guidance.</td>
<td>September 30, 2019</td>
</tr>
<tr>
<td>Updated metrics topics</td>
<td>Improved the descriptions of the real-time metrics definitions. Added categories to the historical metrics definitions.</td>
<td>August 30, 2019</td>
</tr>
<tr>
<td>Updated historical metrics report section</td>
<td>Added categories to the historical metrics definitions.</td>
<td>August 27, 2019</td>
</tr>
<tr>
<td>Re-organized the content</td>
<td>Re-organized the content so it's task-based.</td>
<td>July 19, 2019</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Added information about the updated Transfer to phone number block</td>
<td>You can use the updated Transfer to phone number block to transfer callers to a phone number external to your Amazon Connect instance, and then optionally resume the flow after the call with the external party ends. For more information, see Resume a flow after transfer.</td>
<td>February 18, 2019</td>
</tr>
<tr>
<td>Adding information about live media streaming for customer audio streams</td>
<td>You can capture customer audio during interactions with your contact center and send it to a Kinesis video stream. For more information, see Set up live media streaming of customer audio.</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Added content about agent queues</td>
<td>You can use agent queues to route calls directly to a specific agent. For more information, see Transfer contacts to a specific agent.</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Added information about using Amazon Connect in the Asia Pacific (Tokyo) Region.</td>
<td>For more information, Claim phone numbers for Amazon Connect in the Asia Pacific (Tokyo) Region.</td>
<td>December 10, 2018</td>
</tr>
<tr>
<td>Added information about how to determine agent ACW time from agent event streams</td>
<td>For more information, see Determine how long an agent spends doing ACW.</td>
<td>October 30, 2018</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Added troubleshooting and best practices</td>
<td><strong>Troubleshooting Issues with the Contact Control Panel (CCP)</strong> covers best practices for agent connectivity using the CCP and troubleshooting connectivity and call quality issues in Amazon Connect.</td>
<td>October 18, 2018</td>
</tr>
<tr>
<td>Added information about service-linked roles in Amazon Connect</td>
<td>For more information, see <a href="#">Use service-linked roles for Amazon Connect</a>.</td>
<td>October 17, 2018</td>
</tr>
<tr>
<td>Added information about queue to queue transfers</td>
<td>You can use the new options of the <strong>Transfer to queue</strong> block to enable transferring calls that are already in a queue to another queue. For more information, see <a href="#">Manage contacts in a queue</a>.</td>
<td>July 31, 2018</td>
</tr>
<tr>
<td>Added information about the <strong>Call phone number</strong> block</td>
<td>Updated the content about flows to include the new <strong>Call phone number</strong> block, including how to use the block in a flow. For more information, see <a href="#">Outbound caller ID number</a>.</td>
<td>July 2, 2018</td>
</tr>
<tr>
<td>Added information about contact attributes and the <strong>Get queue metrics</strong> block</td>
<td>For more information, see <a href="#">Use Amazon Connect contact attributes</a>.</td>
<td>June 18, 2018</td>
</tr>
<tr>
<td>Added information about new metrics sent to Amazon CloudWatch Logs.</td>
<td><a href="#">Monitoring your instance using CloudWatch</a> includes additional metrics.</td>
<td>April 19, 2018</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Added information about using SAML for identity management</td>
<td>You can configure your instance to use SAML for identity management. You can also use SAML to enable single sign-on. For more information, see <a href="#">Configure SAML with IAM for Amazon Connect</a>.</td>
<td>March 30, 2018</td>
</tr>
<tr>
<td>Added information about agent call transfers</td>
<td>You can enable call transfers from an agent to another agent, to a queue, or to an external number.</td>
<td>December 10, 2017</td>
</tr>
<tr>
<td>Added information about manager listen-in</td>
<td>You can configure and enable a manager to listen in on agent calls. For more information, see <a href="#">Set up live monitoring for voice and/or chat</a>.</td>
<td>December 10, 2017</td>
</tr>
<tr>
<td>Added information about flow logs</td>
<td>For more information, see <a href="#">Enable flow logs</a>.</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about flow import/export</td>
<td>For more information, see <a href="#">Import/export flows</a>.</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about agent event streams</td>
<td>For more information, see <a href="#">Amazon Connect agent event streams</a>.</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about porting your current phone number to Amazon Connect</td>
<td>For more information, see <a href="#">Port your current phone number to Amazon Connect</a>.</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Added information about</td>
<td>For more information, see</td>
<td>November 1, 2017</td>
</tr>
<tr>
<td>Login/Logout reports</td>
<td>Login/Logout reports.</td>
<td></td>
</tr>
<tr>
<td>Initial release</td>
<td>Initial release of the <em>Amazon Connect Administrator Guide</em>.</td>
<td>March 28, 2017</td>
</tr>
</tbody>
</table>
Amazon Connect Glossary

Channel

How a customer contacts your business: voice (a phone call), chat (a web site or app), and task.

Contact attribute

A piece of data about a contact. You can use this data to personalize the customer experience, make routing decisions about contacts as they progress through your contact center or retrieve real-time metrics about the queues and agents in your contact center to dynamically route contacts based on queue and agent availability.

Flow

Flows define the experience your customers have when they interact with your contact center. These are similar in concept to Interactive Voice Response (IVR). Flows are comprised of blocks, with each block defining a step or interaction in your contact center. For example, there are blocks to play a prompt, get input from a customer, branch based on customer input, or invoke an Lambda function or Amazon Lex bot.

Instance

A virtual contact center. It is 100% cloud-based and can scale to support any sized business. An Amazon Connect instance is not aligned to an EC2 instance or any other hardware concept.

Letter of Authorization

Letter of Authorization (LOA) is a legal document in which you assert to the carrier for Amazon Connect that you have the authority to port phone numbers from your current carrier to the carrier for Amazon Connect. Traditionally, this is a paper document requiring an actual signature.
Losing carrier

Also the customer's current carrier. This is the carrier that currently owns the telephone number. The losing carrier will review all information presented on the Letter of Authorization (LOA) and will validate if it matches the information that they have on file for the customer.

Mutually agreed date and time

After the LOA has been approved by the losing carrier, the losing and winning carriers agree upon a date and time to perform the porting activity.

Omnichannel

A unified contact experience across multiple communication channels, such as voice and chat. Admins can build experiences once, and enable them for voice and chat. Managers monitor and adjust queues from one dashboard. Agents handle all customers using one interface.

Phone number portability

Number portability allows telephone customers to transfer their numbers to other carriers. Carriers and countries may have unique processes and procedures required.

Queue

A waiting area that holds contacts to be answered by agents.

Winning carrier

Also the carrier for Amazon Connect. This is the carrier that the phone number is being ported to, and will own the phone number after the porting is completed.