Amazon Connect
Administrator Guide
## Table of Contents

What is Amazon Connect? .................................................................................................................. 1
Services to use with Amazon Connect .................................................................................................. 1
  Development ................................................................................................................................. 2
  Storage ........................................................................................................................................... 2
  Database ........................................................................................................................................ 3
  Analytics ......................................................................................................................................... 3
  Machine Learning (ML) and Artificial Intelligence (AI) ................................................................. 3
  Messaging ...................................................................................................................................... 3
  Security ........................................................................................................................................ 4
  Management ................................................................................................................................. 4
Supported browsers ............................................................................................................................ 5
  Mobile browsers .......................................................................................................................... 5
Supported languages .......................................................................................................................... 5
  Contact Control Panel .................................................................................................................. 5
  Chat message content ................................................................................................................... 5
  Amazon Connect Admin console .................................................................................................. 6
  Contact Lens for Amazon Connect .............................................................................................. 6
  Amazon Lex .................................................................................................................................. 6
  Amazon Polly .............................................................................................................................. 6
Get started ......................................................................................................................................... 7
  Next steps .................................................................................................................................... 7
Concepts ........................................................................................................................................... 8
  Telephony ..................................................................................................................................... 8
    Telephony architecture .............................................................................................................. 9
    Toll-free numbers ....................................................................................................................... 9
    Direct-in-dial (DID) numbers .................................................................................................... 9
    Claiming numbers in Amazon Connect ................................................................................... 10
    Porting numbers ....................................................................................................................... 10
    Use cases for different configurations .................................................................................... 10
Chat .................................................................................................................................................. 11
  Example chat scenario .................................................................................................................. 11
  When do chats end? ....................................................................................................................... 12
  Enabling your app for chat ........................................................................................................... 13
  Chat initiation method: API .......................................................................................................... 13
  More information .......................................................................................................................... 13
Routing profiles ................................................................................................................................... 14
  Default routing profile: Basic routing profile .............................................................................. 14
  Routing Profiles Link Queues and Agents .................................................................................. 14
Queues: standard and agent .............................................................................................................. 15
  Queues in metrics reports ........................................................................................................... 15
    Default queue: BasicQueue ....................................................................................................... 17
Queues: priority and delay .................................................................................................................. 17
  Example 1: Different priority but same delay ............................................................................ 17
  Example 2: Same priority but different delay ............................................................................ 18
  Example 3: Different Priorities and Delays ............................................................................... 18
  Example 4: Same Priority and Delay ....................................................................................... 18
Queue-based routing .......................................................................................................................... 19
Channels and concurrency ................................................................................................................. 19
Contact flows .................................................................................................................................... 20
  Default contact flows ................................................................................................................... 20
  Contact flow designer ................................................................................................................. 20
Best practices ...................................................................................................................................... 22
Contact flows .................................................................................................................................... 22
User access and security profiles ...................................................................................................... 23
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lambda</td>
<td>23</td>
</tr>
<tr>
<td>Chat and Amazon Lex</td>
<td>23</td>
</tr>
<tr>
<td>Contact Control Panel</td>
<td>23</td>
</tr>
<tr>
<td>Tutorials</td>
<td>25</td>
</tr>
<tr>
<td>Tutorial 1: Set up your Amazon Connect instance</td>
<td>25</td>
</tr>
<tr>
<td>Step 1: Launch Amazon Connect</td>
<td>26</td>
</tr>
<tr>
<td>Step 2: Create an instance</td>
<td>27</td>
</tr>
<tr>
<td>Step 3: Claim a phone number</td>
<td>31</td>
</tr>
<tr>
<td>Tutorial 2: Test the sample voice and chat experience</td>
<td>33</td>
</tr>
<tr>
<td>Step 1: Handle a voice contact</td>
<td>34</td>
</tr>
<tr>
<td>Step 2: Handle a chat contact</td>
<td>38</td>
</tr>
<tr>
<td>Tutorial 3: Create an IT help desk</td>
<td>40</td>
</tr>
<tr>
<td>Step 1: Create an Amazon Lex bot</td>
<td>41</td>
</tr>
<tr>
<td>Step 2: Add permissions to Amazon Lex bot</td>
<td>50</td>
</tr>
<tr>
<td>Step 3: Set up routing</td>
<td>52</td>
</tr>
<tr>
<td>Step 4: Create a contact flow</td>
<td>57</td>
</tr>
<tr>
<td>Step 5: Assign the contact flow to the phone number</td>
<td>69</td>
</tr>
<tr>
<td>Step 6: Test a custom voice and chat experience</td>
<td>71</td>
</tr>
<tr>
<td>Plan identity management</td>
<td>74</td>
</tr>
<tr>
<td>Use an existing directory for identity management</td>
<td>74</td>
</tr>
<tr>
<td>Configure SAML with IAM for Amazon Connect</td>
<td>75</td>
</tr>
<tr>
<td>Important notes</td>
<td>75</td>
</tr>
<tr>
<td>Overview of using SAML with Amazon Connect</td>
<td>75</td>
</tr>
<tr>
<td>Enabling SAML-based authentication for Amazon Connect</td>
<td>76</td>
</tr>
<tr>
<td>Select SAML 2.0-based authentication during instance creation</td>
<td>77</td>
</tr>
<tr>
<td>Enable SAML federation between your identity provider and AWS</td>
<td>77</td>
</tr>
<tr>
<td>Use a destination in your relay state URL</td>
<td>79</td>
</tr>
<tr>
<td>Add users to your Amazon Connect instance</td>
<td>79</td>
</tr>
<tr>
<td>SAML user logging in and session duration</td>
<td>80</td>
</tr>
<tr>
<td>Troubleshoot SAML with Amazon Connect</td>
<td>80</td>
</tr>
<tr>
<td>Error Message: Access Denied. Your account has been authenticated, but has not been onboarded to this application</td>
<td>81</td>
</tr>
<tr>
<td>Error Message: Bad Request. The request was not valid and could not be processed</td>
<td>82</td>
</tr>
<tr>
<td>Error Message: Access denied, Please contact your AWS account administrator for assistance</td>
<td>83</td>
</tr>
<tr>
<td>Set up your contact center</td>
<td>85</td>
</tr>
<tr>
<td>Create an Amazon Connect instance</td>
<td>85</td>
</tr>
<tr>
<td>Things to know before you begin</td>
<td>85</td>
</tr>
<tr>
<td>Step 1: Identity management</td>
<td>85</td>
</tr>
<tr>
<td>Step 2: Administrator</td>
<td>86</td>
</tr>
<tr>
<td>Step 3: Telephony options</td>
<td>86</td>
</tr>
<tr>
<td>Step 4: Data storage</td>
<td>87</td>
</tr>
<tr>
<td>Step 5: Review and create</td>
<td>87</td>
</tr>
<tr>
<td>Next steps</td>
<td>88</td>
</tr>
<tr>
<td>Create a test instance</td>
<td>88</td>
</tr>
<tr>
<td>Find your instance ID</td>
<td>88</td>
</tr>
<tr>
<td>Update instance settings</td>
<td>89</td>
</tr>
<tr>
<td>Enable data streaming</td>
<td>91</td>
</tr>
<tr>
<td>Emergency admin login</td>
<td>92</td>
</tr>
<tr>
<td>Delete your instance</td>
<td>93</td>
</tr>
<tr>
<td>Test a voice or chat experience</td>
<td>93</td>
</tr>
<tr>
<td>Set up your phone numbers</td>
<td>94</td>
</tr>
<tr>
<td>Claim a phone number in your country</td>
<td>95</td>
</tr>
<tr>
<td>Claim a phone number you already own in another country</td>
<td>95</td>
</tr>
<tr>
<td>Request international numbers or special numbers</td>
<td>96</td>
</tr>
<tr>
<td>Release a phone number</td>
<td>96</td>
</tr>
<tr>
<td>Port your current phone number</td>
<td>97</td>
</tr>
<tr>
<td>Claim phone numbers for Asia Pacific (Tokyo)</td>
<td>101</td>
</tr>
</tbody>
</table>
Region requirements for phone numbers ................................................................. 103
Set up routing ........................................................................................................ 118
  How routing works ............................................................................................... 119
  Create a queue ..................................................................................................... 120
  Disable a queue .................................................................................................... 120
  Set queue capacity ............................................................................................... 121
  Set the hours of operation ................................................................................... 122
  Set up outbound caller ID ................................................................................... 124
  Create a routing profile ....................................................................................... 126
  Set up queue-based routing ................................................................................ 128
Set up agents .......................................................................................................... 128
  Set up agent hierarchies ..................................................................................... 129
  Customize agent status ....................................................................................... 130
  Configure agent settings ..................................................................................... 131
  Enable auto-accept call ..................................................................................... 132
  Set up automatic agent logout ......................................................................... 133
Upgrade to the latest CCP ....................................................................................... 134
  Upgrade on your own schedule, before your automatic upgrade date ............. 135
  Upgrade later, automatically ............................................................................. 135
  My CCP URL ends with /ccp# ............................................................................ 135
  I use the Amazon Connect Streams API ............................................................ 146
Provide access to the CCP .................................................................................... 148
  Grant microphone access in Chrome or Firefox ................................................... 148
  How to get help for CCP issues .......................................................................... 148
  Headset and workstation requirements .............................................................. 148
  Can't hear caller or caller can't hear agent? ......................................................... 150
  Can't hear indicator for incoming chat? ............................................................... 150
Create contact flows ................................................................................................ 152
  Default contact flows .......................................................................................... 152
    Change a default contact flow ............................................................................ 153
    Default agent hold ............................................................................................. 156
    Default agent transfer ....................................................................................... 156
    Default customer queue .................................................................................... 156
    Default customer whisper ................................................................................ 159
    Default agent whisper ...................................................................................... 159
    Set the default whisper flow for chat ............................................................... 159
    Default customer hold ...................................................................................... 160
    Default outbound .............................................................................................. 160
    Default queue transfer ...................................................................................... 161
    Default prompts from Amazon Lex ................................................................. 161
Sample contact flows ............................................................................................... 161
  Sample inbound flow ........................................................................................... 162
  Sample AB test .................................................................................................... 162
  Sample customer queue priority ........................................................................ 163
  Sample disconnect flow ...................................................................................... 163
  Sample queue configurations ............................................................................ 163
  Sample queue customer ..................................................................................... 166
  Sample queued callback .................................................................................... 167
  Sample interruptible queue flow with callback .................................................. 167
  Sample Lambda integration ................................................................................ 168
  Sample recording behavior ................................................................................. 168
  Sample note for screenpop .................................................................................. 168
  Sample secure input with agent ......................................................................... 169
  Sample secure input with no agent .................................................................... 169
Create a new contact flow ....................................................................................... 169
  Before you begin: develop a naming convention ............................................... 170
  Choose a contact flow type ................................................................................ 170
Create an inbound contact flow ................................................................. 171
Generate logs .......................................................................................... 172
Copy and paste contact flows ................................................................. 172
Roll back a contact flow ........................................................................... 173
Associate a phone number with a contact flow ...................................... 173
Create prompts ....................................................................................... 173
  Maximum length for prompts .............................................................. 174
  Bulk upload of prompts ....................................................................... 174
  Add text-to-speech to prompts ............................................................. 174
  Choose the voice for audio prompts .................................................. 176
  Use SSML tags to personalize text-to-speech ...................................... 176
  SSML tags aren’t interpreted in chats ................................................... 177
  SSML tags supported by Amazon Connect ........................................... 178
Set up contact transfers ......................................................................... 178
  Overview of steps ................................................................................ 179
  Create quick connects ......................................................................... 179
  Delete quick connects ......................................................................... 180
  How quick connects work ..................................................................... 181
  Set up agent-to-agent transfers ........................................................... 183
  Resume a contact flow after transfer .................................................. 186
  Manage contacts in a queue ............................................................... 187
  Transfer contacts to agent queue ....................................................... 188
Set up recording behavior ....................................................................... 190
  When is a conversation recorded? ....................................................... 190
  Where are recordings stored? ............................................................. 190
  When are recordings available? .......................................................... 191
  How to set up recording behavior ...................................................... 191
  How to set up users ............................................................................. 191
Set up queued callback .......................................................................... 191
  Steps to set up queued callback ........................................................ 192
  Create a contact flow for queued callbacks ........................................ 192
  Learn more about queued callbacks ................................................. 196
Import/export contact flows .................................................................... 197
  Export limitations .............................................................................. 197
  Contact flows are exported to JSON files ......................................... 197
  How to import/export contact flows .................................................. 197
  Resolve resources in imported contact flows ....................................... 198
Track events in contact flows .................................................................. 198
  Storage for contact flow logs ............................................................. 199
  Enable contact flow logs .................................................................... 199
  Data in contact flow logs .................................................................... 200
  Track customers between contact flows ............................................ 201
  Create alerts for contact flow log events ............................................ 201
Contact block definitions ....................................................................... 201
  Call phone number ........................................................................... 203
  Change routing priority / age ............................................................. 205
  Check contact attributes .................................................................... 207
  Check hours of operation ................................................................... 210
  Check queue status ........................................................................... 211
  Check staffing .................................................................................... 213
  Disconnect / hang up .......................................................................... 215
  Contact flow types ............................................................................. 215
  Distribute by percentage ..................................................................... 215
  End flow / Resume .............................................................................. 217
  Get customer input ............................................................................ 218
  Get queue metrics .............................................................................. 225
  Hold customer or agent ...................................................................... 230
<table>
<thead>
<tr>
<th>Release Date</th>
<th>Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2018 Updates</td>
<td>New Features, General, Metrics and Reporting, Contact Flows</td>
</tr>
<tr>
<td>June 2018 Updates</td>
<td>General, Telephony and Voice, Contact Flows, Metrics and Reporting, Contact Control Panel (CCP)</td>
</tr>
<tr>
<td>April and May 2018 Updates</td>
<td>General, Telephony and Voice, Contact Flows, Metrics and Reporting, Contact Control Panel (CCP)</td>
</tr>
<tr>
<td>Administrative support</td>
<td>593</td>
</tr>
<tr>
<td>Document history</td>
<td>594</td>
</tr>
<tr>
<td>Earlier updates</td>
<td>595</td>
</tr>
</tbody>
</table>
What is Amazon Connect?

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.

Amazon Connect is an open platform that you can integrate with other enterprise applications, such as Salesforce. In addition, you can take advantage of the AWS ecosystem to innovate new experiences for your customers.

The following diagram shows these key characteristics of Amazon Connect.

---

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 (p. 339)
- Blog post: Building a state-aware workflow with Amazon Connect and AWS Step 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 (p. 87) in Create an Amazon Connect instance (p. 85).

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 trace record (CTR) in Amazon Connect. To fix this, use a Lambda function to rename the S3 Glacier object to match the data in the CTR.
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 trace records (CTRs)** (p. 416). CTRs 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 contact flow logs, you can set up an Amazon Kinesis stream to stream your contact flow log data from CloudWatch to a data warehouse service, such as Amazon Redshift. You can combine the contact flow log data with other Amazon Connect data in your warehouse, or run queries to identify trends or common issues with a contact flow.

For more information, see:
- How to access Kinesis Video Streams data (p. 348)
- 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 (p. 332).
- Amazon Polly—Provides text-to-speech in all contact flows. For more information, see Add text-to-speech to prompts (p. 174) and SSML tags supported by Amazon Connect (p. 178).
- 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 (p. 509).
• 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 (p. 74)
• 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 (p. 497).
• AWS CloudFormation—Amazon Connect does not support this directly for creating instances. However, it does support AWS CloudFormation templates for associated services, like integrations, database export, and so on.
• AWS CloudTrail—Provides a record of Amazon Connect API calls. This is especially useful for tracking who accessed recorded conversations (p. 373).

For more information about Amazon Connect and AWS CloudTrail, see Logging Amazon Connect API calls with AWS CloudTrail (p. 502).

Browsers supported by Amazon Connect

Agents use the Contact Control Panel (CCP) (p. 536) in Amazon Connect to communicate with contacts. The CCP is a website that they access using a web browser.

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>Mozilla Firefox ESR</td>
<td>Latest three versions</td>
<td>Open Firefox. On the menu, choose the Help icon and</td>
</tr>
</tbody>
</table>
For more requirements, see Agent headset and workstation requirements for the CCP (p. 148).

**Browsers on mobile devices**

The Amazon Connect console and Contact Control Panel (CCP) do not work on mobile browsers.

**Languages supported by Amazon Connect**

**Contact Control Panel**

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

- Chinese (Simplified)
- English
- French
- German
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

Contact Lens for Amazon Connect

- English (Australia)
- English (India)
- English (Great Britain)
- English (United States)
- Spanish (Spain)
- Spanish (United States)

Amazon Lex

See Languages Supported in Amazon Lex in the Amazon Lex Developer Guide.

Amazon Polly

See Voices in Amazon Lex in the Amazon Polly Developer Guide.
Get started with Amazon Connect

Use these steps to set up your contact center.

1. Create an Amazon Connect instance (p. 85). Use an instance to contain all the resources and settings related to your contact center. You specify where voice recordings and chat transcripts are stored, and how you plan to manage user accounts and other aspects.

2. Set up phone numbers for your contact center (p. 94). 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 (p. 118). 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, or both. You also specify how many chats an agent can manage at the same time.

4. Create Amazon Connect contact flows (p. 152). Establish a contact flow to define the customer experience with your contact center from start to finish. A single contact flow works for both voice and chat, which makes your design more efficient. When you build contact flows and configure the blocks, indicate how the flow should work for voice, chat, or both.

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 (p. 357) and Set up agents (p. 128).

6. If you're using chat, enable your customer-facing app to engage with Amazon Connect chat. For an example on GitHub, click here.

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 (p. 190). 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 contact flows. For chat conversations, set up recording at the instance level.

   To learn how to monitor conversations, see Monitor live conversations (p. 367).

2. Add an Amazon Lex bot (p. 332). 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.
Concepts

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

In Amazon Connect you build once and enable the experience for both voice and chat channels:

- You use the same routing profiles, queues, contact flows, metrics, and reports for both channels.
- Managers monitor both 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 two.

Contents
- Telephony (p. 8)
- Chat (p. 11)
- Routing profiles (p. 14)
- Queues: standard and agent (p. 15)
- Queues: priority and delay (p. 17)
- Queue-based routing (p. 19)
- Channels and concurrency (p. 19)
- Contact flows (p. 20)

Telephony

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 Amazon Connect provides for telephony, which will help you build a solution to meet your business requirements.

Contents
- Telephony architecture (p. 9)
- Toll-free numbers (p. 9)
- Direct-in-dial (DID) numbers (p. 9)
- Claiming numbers in Amazon Connect (p. 10)
- Porting numbers (p. 10)
- Use cases for different configurations (p. 10)
**Telephony architecture**

Amazon Connect provides capabilities to host both toll-free and direct dial numbers (DID) in all regions supported by Amazon Connect. You can use both types of numbers in a single instance. A complete list of supported countries and costs, including the price differences between DID and toll-free numbers can be found 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 leverage 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.

**Toll-free numbers**

Toll-free numbers are telephone 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 toll-free numbers are managed and distributed in accordance with local laws.

AWS manages toll-free numbers as a Responsible Organization, or “RespOrg.” When you claim or port a number into Amazon Connect, we register that number with SOMOS. Once 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 toll-free numbers are a higher price than direct dial, but the service reliability and customer experience makes this the most attractive option.

**Direct-in-dial (DID) 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 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 a toll-free number. The ability to localize numbers may be an attractive option for your business.

**Claiming numbers in Amazon Connect**

Amazon Connect provides you the ability to claim both direct dial and toll-free numbers in supported countries from inventories maintained by AWS. To claim a number, log into your Amazon Connect instance and select **Phone numbers**. For instructions, see Claim a phone number in your country (p. 95).

**Porting numbers**

Porting of numbers refers to the ability to move an existing telephone number from one carrier to another provided you are the “customer-of-record.” In the United States, portability is required and regulated by the Federal Communications Commission. Laws regarding the requirements for number portability vary greatly between countries. In the United States and Canada, the process is regulated and well-defined. In other countries, some have very well-defined processes while some are dependent on carrier and geography.

If you are trying to port a number outside of the United States, follow the porting process (p. 97) we’ve documented, however, the timeline to complete may vary. If porting is not possible at all, AWS support will let you know that it’s not available.

To begin the porting process, you will need to gather some documentation to enable the process to run smoothly. AWS support will need a copy of your bill showing the current carrier, number(s) to port, and the company name. Feel free to redact any pricing or company information you feel is proprietary. You will also need to provide your Amazon Connect instance ID.

For detailed porting instructions, see Port your current phone number (p. 97).

**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 Claim a phone number in your country (p. 95).

**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.
- Once fully converted, use the porting process (p. 97) 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 contact flows to transfer calls to the other platform on a telephone number you will
provide in the contact flow.
• If the third-party 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 use case we recommend you engage AWS Solution Architecture support to ensure your contact
center is well-architected to achieve the best possible outcomes.

Chat

Amazon Connect allows 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. It’s an
asynchronous interaction. Learn more.

Example chat scenario

Suppose a customer and agent are chatting, but then 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 contact flow determines what happens next.

In this scenario let’s say the customer eventually sends another message (“Hey, I’m back”) and the chat
resumes. Depending on the logic you define in the contact flow, the chat can be assigned to the original
agent, or a different agent/queue.

Here’s how you build this scenario:

1. Create a disconnect flow. The following image shows the Sample disconnect flow (p. 163).

2. In the disconnect flow, add a Wait (p. 274) 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/agent.

3. In your inbound contact flow, add the **Set Disconnect Flow** (p. 245) 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** (p. 162).

### When do chats end?

The total duration for a chat conversation, including the time spent waiting when the customer isn't active, can't exceed 25 hours. After that the chat conversation ends.

During the 25 hours, there's no limit to the number of times a customer can stop and resume chat.

To specify wait time shorter than 25 hours, use the **Wait** (p. 274) block. For example, you might wait 12 hours for the customer to resume the chat. 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 shorter wait time, you'll ensure customers have a good experience. Otherwise, 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 automatically 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** in the **Amazon Lex Developer Guide**.
Enabling your app for chat

With only a few steps, you can enable your app to engage with Amazon Connect chat. Use the sample implementation on GitHub to help you get started. Here's how it works:

- It spins up an Amazon API Gateway endpoint that triggers a Lambda function.
- The Lambda function invokes the Amazon Connect Service StartChatConnect API and returns the result from that call.
- After you spin up the AWS CloudFormation stack you can call this API from your app, import the pre-built chat widget, pass the response to the widget, and start chatting.

In addition, see these resources to customize the chat experience:

- 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

Chat initiation method: API

The StartChatConnect API is used to start the chat.

When you start exploring 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 Trace Record (CTR) is API.

After a chat is transferred to an agent, the Contacts Incoming metric is incremented. The CTR for the transfer no longer increments the API, but it does increment Contacts Incoming.

More information

To learn more about chat, check out the following topics:
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 contact flows (p. 152) 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.
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 contact 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 (p. 428), 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 Agents queues table have been added.
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 (p. 449), 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 contact flows (p. 152) 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.

**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>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>
</tbody>
</table>
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 who handle 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 (p. 128).

Channels and concurrency

Agents can be available concurrently on voice and chat channels at the same time. Here's how this works:

Suppose an agent is configured in their routing profile for voice and up to 5 chats. When the agent logs in, they can be routed a chat or a voice call. However, once they are on a voice call, no more voice calls or chats are routed to them until they finish the call.
If the agent accepts a chat first, up to 5 chats will be routed to them, but no voice calls. Once they are done with the chats, they're available for the next contact, which can be voice or chat. To learn more, see How routing works (p. 119).

To learn more about what the agent experiences in the Contact Control Panel when handling multiple chats, see Chat with contacts (p. 541).

Contact flows

A contact flow defines how a customer experiences your contact center from start to finish. At the most basic level, contact 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, contact flows are significantly more powerful than that: you can create dynamic, personalized flows that interact with other AWS services.

Default contact 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 contact 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 contact flows with your own.

For example, say you create a contact 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 contact flow automatically.

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

For a list of all the default contact flows and what they do, see Default contact flows (p. 152).

Contact flow designer

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

Contact blocks

Contact blocks are the building blocks of your contact flows. Each block is designed for a specific function a business might want in a contact center.
The above contact flow uses five blocks:

- **Set working queue.** When the contact comes in, this block assigns it to the BasicQueue.
- **Check hours of operation.** This block checks whether the contact has arrived when the queue is operating.
- **Transfer to queue.** This block transfers the contact to the BasicQueue.
- **Play prompt.** If the queue is not open for business, or there's an error or it's at capacity, this block plays a message "We are not able to take your call right now."
- **Disconnect/hang up.** Every flow ends with this block.

In the above example, what happens when the customer is transferred to queue, but no agents are available to take their call? The **Default customer queue** flow is triggered. It plays music while the contact is waiting in queue.

For a list of the available contact blocks and descriptions about what they do, see **Contact block definitions (p. 201).**

**Sample contact flows**

To see how to put contact blocks together to create different flows, see **Sample contact flows (p. 161).**
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 contact flows, user access and security, Lambda, chat, Amazon Lex, and the Contact Control Panel (CCP).

Contact 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 contact 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 contact flow where sensitive information is collected and can’t be stored in CloudWatch.
- Use Set recording behavior block in your contact 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.
  - Use attribute and value variableName works as expected.
  - Use attribute and $.External.varableName results in a prepended period.
- Before transferring a call to an 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 contact flow logic. Also ensure that for each call, the contact flow connects the caller to an agent, bot, or transferred externally for further assistance.

User access and security profiles

• 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 (p. 92).

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 (p. 287).

• 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, add the CCP URL to the allow list in the agent’s Chrome settings. Otherwise, they won’t hear the audio indicator notifying them that there’s an incoming chat.
For instructions, see this [Google Chrome Help article](https://support.google.com/chrome).
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.

![PDF icon](image)

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 (p. 25)
- Tutorial 2: Test the sample voice and chat experience (p. 33)
- Tutorial 3: Create an IT help desk (p. 40)

**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 (p. 26)
- Step 2: Create an instance (p. 27)
- Step 3: Claim a phone number (p. 31)

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 (p. 27)**.

**Step 2: Create an instance**

1. On the **Amazon Connect virtual contact center instances** page, choose **Add an instance**.
2. Type a unique name for your instance. For example, the following image shows **mytest89** as a name. Choose a different name for your instance. Then choose **Next step**.

3. On the **Create an 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 step**.
4. On the **Telephony Options** page, accept the default settings and choose **Next step**.

5. On next two pages - **Telephony Options** and **Data storage** - accept the default settings, and choose **Next step**.

On the **Data storage** page, accept the default settings, and choose **Next step**.
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. On the left is the navigation menu. Your instance name (also called an alias) displays in the URL.
Congratulations! You set up your instance and now you're on the Amazon Connect dashboard. Go to Step 3: Claim a phone number (p. 31).

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 navigation menu, choose Routing, Phone numbers.
2. On the right side of the page, choose Claim a number.
3. Select the **DID (Direct Inward Dialing)** tab. Use the drop-down arrow to choose your country/region. 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 Contact 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** (p. 33).

### 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)** (p. 536). 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

1. On the navigation menu, choose Dashboard.

2. On the Dashboard page, choose Test chat.

3. 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 **Routing, 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 (p. 162)** 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 contact 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 **Clear contact**. This frees up 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: Handle a chat contact (p. 38)** to experience how to handle a chat contact.

**Step 2: 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. Choose the chat bubble to start a chat.
2. 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.*

3. In the CCP, accept the incoming chat.
4. Use the CCP to send chat messages to the customer.
5. 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 contact flow, and then test the custom voice and chat experience. Go to Tutorial 3: Create an IT help desk (p. 40).

**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 contact 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

**Contents**

- Step 1: Create an Amazon Lex bot (p. 41)
- Step 2: Add permissions to Amazon Lex bot (p. 50)
- Step 3: Set up routing (p. 52)
- Step 4: Create a contact flow (p. 57)
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 (p. 41)
- Part 2: Add intents to your Amazon Lex bot (p. 43)
- Part 3: Add sample utterances (p. 45)
- Part 4: Build and test the Amazon Lex bot (p. 47)
- Part 5: Publish the Amazon Lex bot and create an alias (p. 49)

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 a 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 are already in the Amazon Lex dashboard.

3. Choose Custom bot.
4. Enter the following information:

- **Bot name** — For this tutorial, name the bot **HelpDesk**.
- **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 [Children's Online Privacy Protection Act](https://www.coppa.org/).
5. Choose Create.

Go to Part 2: Add intents to your Amazon Lex bot (p. 43).

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, choose the Editor tab.
2. Choose the + icon next to **Intents**, and choose **Create new intent**.

3. In the **Add intent** box, choose + **Create intent**.

4. Name the intent **PasswordReset** and choose **Add**.
5. Choose the + icon next to **Intents** again, and add an intent for **NetworkIssue**.

Go to the next topic, Part 3: Add Sample Utterances.

**Part 3: Add sample utterances**

After defining the intents, add some sample utterances. Utterances are what a customer might say or chat to the bot.

1. In the Amazon Lex console, select the **PasswordReset** intent.

2. Add the sample utterance *I forgot my password*, and choose the + icon.

3. Add the utterance *reset my password*.

   The sample utterances look like what's shown in the following image.
4. Select the **NetworkIssue** intent.

5. Add a sample utterance, such as **I can't access the internet**, and choose +.

6. Repeat step 5 to add the utterance **my email is down**.

The sample utterances look like what's shown in the following image.
Go to Part 4: Build and test the Amazon Lex bot (p. 47).

Part 4: 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 Chatbot.

3. Test the PasswordReset intent. In the Test Chatbot 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.
Step 1: Create an Amazon Lex bot

Go to Part 5: Publish the Amazon Lex bot and create an alias (p. 49).

Part 5: Publish the Amazon Lex bot and create an alias

Next, publish the bot so you can add it to a contact flow in Amazon Connect.

1. In the Amazon Lex console, choose Publish.

2. In the Publish HelpDesk dialog box, use the drop-down to choose the alias that you created for your bot, such as Test.

3. Choose Publish. The publishing takes a few minutes.
4. When Amazon Lex finishes publishing, choose **Close**.

Well done! You created an Amazon Lex bot that has intents and utterances. Now you can add the bot to Amazon Connect. Go to Step 2: Add permissions to Amazon Lex bot (p. 50).

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

To use a bot in your contact 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 **Contact flows**.
4. Under **Amazon Lex**, use the drop-down arrow to choose **HelpDesk**, and then choose **+ Add Lex Bot**.

**Tip**
Only published Amazon Lex bots appear in the drop-down list.

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

6. Choose the access URL of your instance.
This 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 new queue**.
3. Complete the page, as shown in the following image, to add a queue named **PasswordReset**. When done, choose **Add new queue**.

4. Add a queue named **NetworkIssue**. Complete the **Add new 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 new 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 Routing profile queues section, use the drop-down arrow to search for the queues you just created. Choose NetworkIssue, select Voice and Chat, and then choose Add queue.

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

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 **Add new profile** to save the profile.

12. On the navigation menu, go to **Users, User management**.

13. Select your login name, and choose **Edit**.

14. Use the drop-down arrow to choose the routing profile you created, for example, **Test routing profile**. Choose **Save**.
Step 4: Create a contact flow

Routing is all set up and ready to go.

Although Amazon Connect comes with a set of built-in contact flows (p. 152), you can create your own contact flows to determine how a customer experiences your contact center. The contact 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 contact flow that’s specific to the IT Help Desk experience that you’re creating.

1. On the navigation menu, go to **Routing, Contact flows**.

2. Choose **Create contact flow**.

3. The contact flow designer opens. Enter a name for the contact flow, such as **Test contact flow**.
4. Choose the drop-down arrows to expand the sections to access the blocks in them.

5. Drag the following blocks onto the grid: Set logging behavior (p. 249) (in the Set group), Set voice (p. 251) (in the Set group), and Play prompt (p. 236) (in the Interact group).

6. Use your mouse to drag an arrow from the Start block to the Set logging behavior block.
7. Connect the remaining blocks, as shown in the following image.

8. Choose the **Play prompt** title to open its properties page.

9. Configure the **Play prompt** block, as shown in the following image, and then choose **Save**.
10. Add a Get customer input (p. 218) block and connect to the Play prompt block.

11. Choose the title of the Get customer input (p. 218) block to open the properties page.
12. Configure the **Get customer input** block, as shown in the following images.
13. While still in the **Get customer input** block, choose **Add an intent**.

14. Enter the names of the intents that you created in the Amazon Lex bot. They are case sensitive!
15. Choose **Save**.
16. Add a **Play prompt** block (from the **Interact** group) and connect it to the **PasswordReset** branch.

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

19. 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**.

20. Add a **Disconnect / hang up** block (from the **Terminate/Transfer** group) to the grid. Connect the **Default** and **Error** branches to it.
21. Add a **Set working queue (p. 256)** block (from the **Set** group) to the grid. Connect the **Play prompt**.
22. 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**.

![Diagram showing Set working queue block configuration]

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

25. Connect each of the Set working queue blocks to a Transfer to queue block, as shown in the following image.
26. Drag another Disconnect/hang up block onto the grid. Connect all of the remaining Error and At capacity branches to it.

27. The completed contact flow looks similar to the following image.
Step 5: Assign the contact flow to the phone number

1. On the navigation menu, go to **Routing, Phone Numbers**.
2. Choose your phone number.

---

**Tip**

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

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

If the contact flow doesn't save, double-check that all the branches are connected to blocks. That's the most common reason contact flows don't publish.
3. Use the drop-down box to choose the contact flow you just created, and then choose **Save**.

Everything is all set up! Now you’re ready to test your IT Help Desk. Go to **Step 6: Test a custom voice and chat experience (p. 71)**.
Step 6: Test a custom voice and chat experience

You're ready to try out the Amazon Lex bot, routing, and contact flow. The first step is to tell Amazon Connect which contact 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 contact flow you created, for example, Test contact 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 contact flow that you created.

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.
Step 6: Test a custom voice and chat experience

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.
   
   **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 contact flow (p. 152) named Default customer queue (p. 156).

4. Go to the test CCP and accept the incoming call.
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 contact flow (p. 152) named Default agent whisper (p. 159).

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 (p. 96).
Plan your identity management in Amazon Connect

Before you set up your Amazon Connect instance (p. 85), you should decide how you want to manage your Amazon Connect users. **You cannot change the option you select for identity management after you create the instance.**

If you want to change the option or directory you selected, you can delete the instance and create a new one. When you delete an instance, however, you lose all configuration settings and metrics data for it.

Amazon Connect is integrated with AWS Directory Service. When you create your instance, you'll be prompted to choose from one of the following identity management solutions supported in Amazon Connect:

- **Store users with Amazon Connect**—Choose this option if you want to create and manage user accounts within Amazon Connect. A AWS Directory Service instance will be created in your AWS account.
  
  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 (p. 74).

- **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 (p. 75)

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](https://aws.amazon.com/pricing/details/directory-service).

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 with Security Assertion Markup Language (SAML) 2.0 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). The IdP includes an option to log in to Amazon Connect, which redirects the user to your Amazon Connect instance without having to provide separate credentials for Amazon Connect.

### Important notes

Before you begin, note the following:

- Amazon Connect instance allow only a 1:1 mapping of user roles to SAML authentication.

- To enable SAML authentication, create an AWS Identity and Access Management (IAM) role for federation. The role is used for federation between the your IdP and Amazon Web Services. AWS Identity and Access Management is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources. In this case, the IAM role is used for federation between your identity provider and AWS. The permissions for the IAM role grant access to Amazon Connect.

- You cannot use your root AWS account as the account for SAML federation. Instead, follow the steps in the topic, and the topics linked to in the AWS Identity and Access Management documentation, to create an IAM role for federation. To learn more about IAM, see [What is IAM?](https://aws.amazon.com/identity-access-management/what-is-iam/)

### Overview of using SAML with Amazon Connect

The following diagram shows the flow for SAML requests to authenticate users and federate with Amazon Connect.
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. The user names must exactly match the user name in your network directory and your identity provider.
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).

   **Important**
   Replacing this role causes previously federated users to fail at federation because it breaks existing user logins.

   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:

```json
{
    "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.

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

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) 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.

4. Configure SAML Assertions for the Authentication Response. For more information, Configuring SAML Assertions for the Authentication Response.

5. 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:

https://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.

**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

### 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:

https://us-east-1.console.aws.amazon.com/connect/federate/instance-id?
destination=%2Fconnect%2Fccp-v2

### 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, by default, 10 hours.

About session expiration

Amazon Connect sessions expire 10 hours after a user logs in. After 10 hours, users are automatically logged out, even if they are currently on a call. If your agents stay logged in for more than 10 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.

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.
Error Message: Access Denied. Your account has been authenticated, but has not been onboarded to this application.

What does this mean?

This error means that the user has successfully authenticated via 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.

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:

   ```
   $ 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:

   ```
   $ cat samlresponse.txt | python3 -c "import sys; from urllib.parse import unquote; print(unquote(sys.stdin.read()));" | base64 --decode > samlresponsedecoded.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:
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).

This is the returned RoleSessionName

### Error Message: Bad Request. The request was not valid and could not be processed.

### What does this mean?

One of the most common reasons for this error is an Amazon Connect user logged in previously using a different identity provider. For example, first they logged in using this attribute name:

```xml
<Attribute Name="https://aws.amazon.com/SAML/Attributes/Role"/>
```

Then the same user tried to login but with a different `Role` SAML Attribute, for example:
Error Message: Access denied, Please contact your AWS account administrator for assistance.

Resolution

• If you need to change the Amazon Connect user to the new role then you need to delete and recreate the user in the Amazon Connect instance. For instructions for doing this in Amazon Connect console, see Manage users in Amazon Connect (p. 357). Or, use these commands:

  1. Get the user ID:
     ```bash
     aws connect list-users --instance-id [INSTANCE_ID]
     ```
  2. Delete the user:
     ```bash
     aws connect delete-user --instance-id [INSTANCE_ID] --user-id [USER_ID]
     ```
  3. Use the Amazon Connect console or the CLI to create the user account.

• If you don’t need to change the user to the new role, double-check the IdP settings to make sure that the user logs in using the old role instead.

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 via 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:

```
$ aws iam attach-role-policy --role-name [ASSUMED_ROLE] --policy_arn [POLICY_WITH_GETFEDERATIONTOKEN]
```
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 (p. 7).

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 contact 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 (p. 85)
- Test a voice or chat experience (p. 93)
- Set up phone numbers for your contact center (p. 94)
- Set up routing (p. 118)
- Set up agents (p. 128)
- Upgrade to the latest CCP (p. 134)
- Provide access to the Contact Control Panel (p. 148)

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 an IAM user to create an instance, ensure that they have the permissions granted by the AmazonConnectFullAccess policy.
- 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 (p. 74).

Step 1: Identity management

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 (p. 74).

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 within Amazon Connect** - Use Amazon Connect to create and manage user accounts.
   - **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.

Step 2: 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 Add a new admin, 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.

Step 3: Telephony options

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.

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 using the option described in this procedure.
To configure telephony options for your instance

1. (Optional) To enable customers to call into your contact center, choose I want to handle incoming calls with Amazon Connect.
2. (Optional) To enable outbound calling from your contact center, choose I want to make outbound calls with Amazon Connect.
3. (Optional) To enable agents to hear pre-connection audio such as busy signals or “This phone number has been disconnected and is no longer in service,” choose I want to enable early media.

Step 4: Data storage

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.

By default, Amazon Connect creates buckets for storing call recordings, chat transcripts, exported reports, and contact 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 (p. 190).
- 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 (p. 190).
- Live media streaming is not enabled by default.

To customize the data storage settings for your instance or enable/disable certain functionality:

1. Choose Customize settings.
2. (Optional) To specify the bucket and KMS key for recordings of voice conversations, choose Call recordings, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
3. (Optional) To specify the bucket and KMS key for recordings (transcripts) of chat conversations, choose Chat transcripts, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
4. (Optional) To specify the bucket and KMS key for exported reports, choose Exported reports, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
5. (Optional) To disable contact flow logs, clear Enable Contact flow logs.
6. Choose Next step.

Step 5: Review and create

When you are finished configuring your instance, you can create it.

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 Change.

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 (p. 88).

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 for your contact center (p. 94).

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
There's no way to migrate all resources between virtual contact center instances. You can migrate some instance resources manually or with the assistance of AWS Support. Other resources must be recreated.
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 (p. 85).

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, click on the instance alias. The instance alias is also your instance name, which appears in your Amazon Connect URL. For example, in https://mytest88.awsapps.com/connect/home the instance name is mytest88.
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. For example, in https://mytest88.awsapps.com/connect/home the instance name is mytest88.
3. Complete the following procedures.

Update telephony options

1. In the navigation pane, choose Telephony.
2. (Optional) To enable customers to call into your contact center, choose **I want to handle incoming calls with Amazon Connect**.

3. (Optional) To enable outbound calling from your contact center, choose **I want to make outbound calls with Amazon Connect**.

4. (Optional) 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 **I want to enable early media**.

5. Choose **Save**.

**Update data storage**

1. In the navigation pane, choose **Data storage**.

2. (Optional) To specify the bucket and KMS key for recordings of voice conversations, choose **Call recordings**, **Edit**, specify the bucket name and prefix, select the KMS key by name, 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 contact flow (p. 190)**.

3. (Optional) To specify the bucket and KMS key for recordings (transcripts) of chat conversations, choose **Chat transcripts**, **Edit**, specify the bucket name and prefix, select the KMS key by name, 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.

4. (Optional) To enable live media streaming, choose **Live media streaming**, **Edit**. For more information, see **Capture customer audio: live media streaming (p. 346)**.

5. (Optional) To specify the bucket and KMS key for exported reports, choose **Exported reports**, **Edit**, specify the bucket name and prefix, select the KMS key by name, and then choose **Save**.

**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 (p. 91)**.

3. For **Contact Trace 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 contact flow settings**

1. In the navigation pane, choose **Contact flows**.

2. (Optional) To add a signing key for use in contact flows, choose **Add key**. For more information, see **Encrypt customer input (p. 344)**.

3. (Optional) To integrate with Amazon Lex, select a Lex bot. For more information, see **Add an Amazon Lex bot (p. 332)**.
4. (Optional) To integrate with AWS Lambda, select a Lambda function. For more information, see *Invoke AWS Lambda functions* (p. 339).

5. (Optional) To enable contact flow logs, choose **Enable contact flow logs**. For more information, see *Track events as customers interact with contact flows* (p. 198).

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* (p. 174).

---

### Enable data streaming for your instance

You can export contact trace records (CTRs) 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. For example, in [https://mytest88.awsapps.com/connect/home](https://mytest88.awsapps.com/connect/home) the instance name is *mytest88*.
3. In the navigation pane, choose **Data streaming**.
4. Choose **Enable data streaming**.
5. For **Contact Trace 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.
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 master key (CMK) to use for encryption.
3. Choose the same CMK 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:

- Login in at https://name_of_instance.awsapps.com/connect/login

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.
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 instance**
If you no longer want to use an instance, you can delete it. When you delete an instance, the phone number claimed for the instance is released back to inventory. You lose all settings, data, metrics, and reports associated with the instance. When customers call the phone number you've released, they'll get a message that it's not a working phone number.

**Important**
You cannot undo the deletion of an instance or restore settings or data from the instance after it is deleted.

**To delete an instance**
1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Select the check box for the instance and choose Remove.
3. When prompted, type the name of the instance and choose Remove.

**Test a voice or chat experience**
To learn what the voice and chat experiences are like for your agents and customers, you can test them without doing any development.

**To test voice:** once 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 contact flows (p. 152) to power your initial experience. To test a customized contact flow, assign a phone number (p. 173) to it and then call that number.

**To 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. Go to the Amazon Connect Dashboard, and choose **Test chat**.

   If you don't see the option to test chat, click here.

2. On the **Test Chat** page, choose **Test Settings**.

3. Under **System Settings**, choose the contact flow you want to test with chat, and then click **Apply**. By default, it runs the **Sample inbound flow** (p. 162).

4. In the chat window, click the icon as shown below.

5. Type a message similar to what one of your customers might type. In the agent window, type a reply.

6. 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 (p. 126).

   To learn more about what the agent experiences when managing chat conversations, see Chat with contacts (p. 541).

---

**Set up phone numbers for your contact center**

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 into your contact center to confirm that it is working correctly. You can also use it in your production environment.

For pricing information about how much a claimed phone number costs, see Amazon Connect pricing.

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 contact flows.

**Contents**

- Claim a phone number in your country (p. 95)
- Claim a phone number you already own in another country (p. 95)
- Request international numbers, special numbers, or termination points (p. 96)
Claim a phone number in your country

To place or receive calls in your instance, you need to claim a phone number. If you did not claim a number when you created the instance, follow these steps to claim one now.

To claim a number for your contact center

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Routing, Phone numbers.
3. Choose Claim a number. You can choose a toll free number or a Direct Inward Dialing (DID) number.
   
   Note
   Use the Amazon Connect service quotas increase form for these situations:
   
   • If you select a country, but there are no numbers displayed for that country, you can request additional numbers for the country.
   • 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 Contact flow / IVR.
5. Choose Save.
6. Repeat this process until you have claimed all your required phone numbers.

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 (p. 566). If you reach your quota, but want a different phone number, you can release one of 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.

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, see Request international numbers, special numbers, or termination points (p. 96).

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.

**Request international numbers, special numbers, or termination points**

**Important**
To purchase and own a phone number, country regulations often require:

- A local office address
- Specific identification documents

For identification requirements by country, see Region requirements for phone numbers (p. 103).

It can take 2-6 weeks for us to fulfill your request.

To request international phone numbers, special numbers, or termination points, create a support case.

1. Go to Create case.
2. Choose Service limit increase.
3. In Limit type select Amazon Connect.
4. In Use case description, enter the number you want to request.
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.

**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.

**Release a phone number**

If you want a different phone number, or have extra you aren't using you can release them back to inventory.

You cannot claim the same phone number after releasing it.
**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 trigger your contact flows. You may also want to delete your instances. (p. 93)

**To release a phone number**

1. Log in to your contact center using your access URL (https://instance name.awsapps.com/connect/login). To find the name of your instance, see Find your Amazon Connect instance ID/ARN (p. 88).
2. Choose **Routing**, **Phone numbers**.
3. Choose the phone number you want to release, and then choose **Release**.

If the phone number is associated with a contact flow, that flow will be deactivated until another number is associated with it.

When customers call the phone number you've released, they'll get a message that it's not a working phone number.

**Port your current phone number**

To continue using your current phone number with Amazon Connect, you can submit a support ticket to port the number to Amazon Connect. The Amazon Connect team processes your request and assists you with the number porting process.

**How long does it take to port numbers?**

We recommend opening porting requests well in advance of pending go-live dates.

- Porting US or Canada phone numbers usually takes between two to four weeks after you submit the required information.
- Porting non-US phone numbers takes more than two weeks and possibly up to three months, depending on the country. For example, most European countries take about two weeks.
- The amount of time it takes to port numbers depends on the complexity of the request and your current carrier. For example:
  - Porting 100 numbers from one carrier is usually faster than porting three numbers from three different carriers.
  - Porting local, direct dial numbers is usually faster than porting toll-free numbers.
- After a number is ported to Amazon Connect, the Support team maps your number to your connect instance for you to map to required flow. You can also request that the Amazon Connect Support team map the number to your contact flow for you.

**How to port your numbers**

When you port your current phone number into Amazon Connect, we provide any possible assistance. Many of the steps, however, are performed by telecommunications carriers.

1. **Submit an Amazon Connect support ticket to port your number.**
   - Submit a port request: Premium support plan instructions (p. 98)
   - Submit a port request: Basic support plan instructions (p. 99)
2. **The Amazon Connect team reviews your ticket.**
   
   We confirm whether the numbers that you request can be ported from your current carrier. We then contact you with next steps, or notify you that the requested numbers cannot be ported. For common reasons, see see Why carriers reject port requests (p. 100).
3. **Complete the Letter of Authorization/Agency (LOA).**

If your number can be ported, we provide you with an LOA form appropriate for the type of number to port. The LOA form authorizes your current carrier to release your number and allow it to be ported.

- If you are porting multiple numbers from different carriers, fill out a separate LOA form for each carrier.
- The name, address, and information you provide on the LOA form must match the information on file with your current carrier exactly. One way you can help ensure the porting process goes smoothly is to include a copy of the Customer Service Record (CSR) from your carrier, which has your name and address on it. Check that the information on your LOA form matches your CSR exactly.

A LOA form has the following information:

- The numbers to port.
- Information about your current carrier, such as a phone bill.
- Contact information for the person authorized to make changes to your phone service.

**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 reject an electronic or printed signature.
- It must be dated within 30 days of when the Amazon Connect Support team submits the LOA to the carrier.
- It must include any toll-free numbers you want to port. Up to 10 toll-free numbers can be listed on the LOA.
- A spreadsheet is required if you are requesting more than 10 toll-free numbers be ported. The LOA should specify “See Attached” and the spreadsheet should be attached to the LOA.
- It must include only those toll-free numbers that belong to the same current carrier. If you have multiple current carriers, you need to submit multiple LOAs.

4. **The Amazon Connect team submits the LOA** to the carrier for Amazon Connect on your behalf.

5. **The new carrier works with your current carrier** to move your current number over to their service.

- If your current carrier is able to validate and approve your request, they provide a date for the number to be ported to Amazon Connect.
- If your current carrier rejects the request to port your number due to the LOA not having correct or complete information, the Amazon Connect team contacts you and requests a new LOA to submit to the carrier.

Every time we resubmit an LOA, there is an additional 3-5 business days of waiting time. Unfortunately, we cannot expedite the LOA acceptance/rejection process. We must wait for a response from your current carrier.

For more information, see Why carriers reject port requests (p. 100).

6. **Amazon Connect contacts you with your porting date.** When we receive a date from your current carrier, we start adding the numbers to your Amazon Connect instance about a day before the scheduled date.

---

**Submit a port request: Premium support plan instructions**

2. In the upper right corner of the page, choose **Support, Support Center**.

3. On the **AWS Support Center** page, choose **Create case**.

4. Choose **Technical Support**.

5. Under **Case classification**, do the following:
   
   a. Choose service as **Connect (Contact center)**.
   
   b. Choose category as **Phone Number Porting**.
   
   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 (p. 88)**.
   
   e. Enter the subject.
   
   f. Under **Case description, Use case 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.

6. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.

7. Choose **Submit**.

8. The Amazon Connect team reviews your ticket, and gets back to you with next steps.

### Submit a port request: Basic support plan instructions

1. Log in to the **AWS Management Console** (https://console.aws.amazon.com/console) using your AWS account.

2. In the upper right corner of the page, choose **Support, Support Center**.

3. On the **AWS Support Center** page, choose **Create case**.

4. Choose **Service limit increase**.

5. Under **Case details**, do the following:
   
   a. For **Limit type**, choose **Amazon Connect**.
b. For **Contact Center Instance ARN - optional**, 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 (p. 88).

6. Under **Requests, Request 1** do the following:
   a. For **Region**, select the Region in which you created your Amazon Connect instance.
   b. For **Limit**, choose **Phone Number Porting**.
   c. For **New limit value**, enter the number of phone numbers to port.

7. (Optional) If you want to port more phone numbers, choose **Add another request**, and then repeat step 6 for each additional request.

8. Under **Case description, Use case description**, include as much information as possible about your request, including whether the numbers are Direct Inward Dial or toll-free, 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 may leave information out.

9. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.

10. Choose **Submit**.

11. The Amazon Connect team reviews your ticket, and gets back to you with next steps.

### Why carriers reject port requests

Following are the most common reasons a port request may be initially rejected by your current 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, contact your carrier to update your CSR information.

  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.

- **Number cannot be ported**

  Some numbers can't be ported due to specific country or carrier limitations. In these situations, consider claiming a new number from Amazon Connect.

### Porting phone numbers in other countries

If you are trying to port a number outside of the United States, follow the same steps for porting numbers, however, the timeline to complete may vary. If porting is not possible at all, AWS support will let you know that it's not available.

### Port phone numbers away from Amazon Connect

To port your number(s) to a different carrier, please open a support case telling us that's what you're going to do. Then make arrangements with your new carrier. By letting us know, it will reduce the amount of back and forth between us and your new carrier, and it will make the process go faster.

1. **Create a case.**
2. **Choose Service limit increase.**
3. In **Limit type** select **Amazon Connect**.

4. In **Use case description**, let us know that you’re porting your number away and the name of your new carrier.

### Claim phone numbers for Amazon Connect in the Asia Pacific (Tokyo) Region

The steps necessary to claim a phone number for an Amazon Connect instance you create in the Asia Pacific (Tokyo) Region are different than the steps to claim a phone number in other AWS Regions. Use the information in this section to claim a phone number for your instance. Amazon Connect does not support porting phone numbers in the Asia Pacific (Tokyo) Region at this time.

### Port and protocol requirements for using Amazon Connect in the Asia Pacific (Tokyo) Region

If your agents use a softphone for Amazon Connect, you must allow traffic in both directions between the network on which the CCP is running and the Amazon Connect for the region in which you created your instance. The required addresses for instances created in the Asia Pacific (Tokyo) Region include the following:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Transport Layer</th>
<th>IP Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>TURN relay media</td>
<td>80 and 443</td>
<td>UDP and TCP</td>
<td>AMAZON_CONNECT ranges in <a href="https://ip-ranges.amazonaws.com/ip-ranges.json">https://ip-ranges.amazonaws.com/ip-ranges.json</a>.</td>
</tr>
</tbody>
</table>

### Using Amazon Connect in the Asia Pacific (Tokyo) Region

Amazon Connect supports 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.

  To claim a number with a 03 prefix, you must provide documentation to verify that you have a physical address in Tokyo. See the next section for more information.

- **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.

**How to claim a phone number for Amazon Connect instances in the Asia Pacific (Tokyo) Region**

You can claim a 050 prefix number directly within Amazon Connect. If you plan to use a number with a 03 prefix from Tokyo, pursuant to Japanese regulatory requirements, you must submit an Amazon Connect service quota increase form to request a number with a 03 prefix for your instance. As part of the approval process, you must provide proof of address documentation to confirm that you have an address in Tokyo. The documents required for address verification are described later in this topic.

While you wait for the request to be processed, you can claim a number with a 050 prefix for your instance. This helps you become familiar with how to configure and use Amazon Connect. When your service quota increase for a 03 prefix number is approved, you can then follow step 6 to search for a “3” prefix number and claim it. After the service quota increase is approved, you will be able to claim additional 03 prefix numbers in the Claim phone number page for that specific account moving forward without opening another support case.

Use these steps to claim a phone number for an instance you create in the Asia Pacific (Tokyo) Region.

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](https://console.aws.amazon.com/connect/).
   You may need to sign in to your AWS account. Confirm that the Region selected is Asia Pacific (Tokyo).
2. On the Amazon Connect console page, choose the Access URL for the instance for which to claim a phone number.
3. Using an account that is assigned the Admin security profile in Amazon Connect, log in to the instance.
4. On the Amazon Connect dashboard, if you have not yet claimed a phone number, follow step 5. If you have already claimed a number, and are claiming an additional number, go to step 6.
5. If you have not yet claimed a number for your instance, choose **Begin** and follow these steps. If you have already claimed a number for your instance, and are claiming an additional number, skip to the next step.
   i. On the Claim phone number page, choose the country from which to claim a phone number.
      Note that only 050 prefix number are available to claim for instances in the Asia Pacific (Tokyo) Region. To claim a 03 prefix number for Tokyo, you must submit a Amazon Connect service quotas increase form.
   ii. Choose the type of number to claim, Direct Dial or Toll Free.
   iii. Choose the phone number to use for your instance from the Phone number drop-down menu.
   iv. Choose **Next**.
      If you see the following message displayed, you must request approval to claim the number selected using the link provided.
      To claim a number in the selected country, please provide a valid business address in that country. Numbers that are claimed without providing a valid local business address may be revoked. To provide the address, please create a support case. Click here to create a support case now.
v. To place a test call to confirm that the number is working correctly with your instance, follow the guidance on the page, or choose Skip for now.

6. If you have already claimed a number for your instance, and are claiming an additional number, choose View phone numbers and then follow these steps.

i. On the Manage Phone numbers page, choose Claim a number.

ii. On the Claim Phone number page, choose the tab for the type of number to claim, Toll free or DID (Direct Inward Dialing).

iii. Select the country from the drop-down menu from which to claim a phone number. Up to five numbers available in that country are displayed. If you want to find a number from a specific prefix, type all or part of the prefix in the Prefix field. If there are numbers with that prefix available, they are displayed on the page.

iv. Choose the number to claim for your instance.

v. Optionally, enter a description for the number to help you identify it later.

vi. To associate the number with a contact flow, choose the flow in the Contact flow / IVR drop-down menu. When you associate a number with a flow, the selected contact flow is invoked when a call comes in to your instance on that phone number.

Proof of address requirements for 03 prefix numbers

When you submit a request to claim a 03 prefix number from Tokyo to use for your Amazon Connect instance, you must provide the following documentation as proof of address due to Japanese regulations as follows:

- If the AWS account used to create the Amazon Connect instance is for an individual, the individual must provide a valid, government-issued identification document, such as a national ID card, passport, or driver's license, with an address visible on the document that matches the city from which the phone number is assigned.

- If the AWS account used to create the instance is for an organization, a representative of the organization must provide the both of the following:
  - A valid, government-issued identification document, such as a national ID card, passport, or driver's license.
  - One of the following documents, with an address visible on the document that matches the city from which the number is assigned. This can be a utility bill, a certificate of company registration from the Ministry of Justice, receipts of payments to a government entity, such as a national or local tax return, or a social security payment receipt.

You can include copies of these documents with your support request for the number, or provide them when requested by AWS Support. After you submit the request, AWS Support reviews it, and then resolves the ticket when address validation is confirmed or if more information is needed. AWS Support will contact you with the results of your request when it is completed. Once AWS Support solves the ticket, and address validation is confirmed you can then follow step 6 above to claim a Tokyo 03 prefix number.

Region requirements for phone numbers

Country 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.

Following is a list of ID requirements by country. When you request an international number (p. 96), we'll work with you to submit your documents.
### Australia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia (AU)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone. Do not use a PO Box.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +61 4</td>
<td>Yes</td>
<td>Proof of the business name, address, and registration number. Also provide a copy of a business license or taxpayer ID certificate. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +61 1300, +61 1800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Austria

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria (AT)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Proof of telecom services at your address, which must match the city code requested.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +43 6</td>
<td>Yes</td>
<td>Your business name, address, the business registration, and a copy of the ID or passport of an authorized representative. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +43 800</td>
<td>Yes</td>
<td>Your business name, address, a copy of the business registration (global), and a copy of the passport of an authorized representative.</td>
</tr>
<tr>
<td>Country Summary</td>
<td>Numbers Summary</td>
<td>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 global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>National prefixes: +43 720</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Belgium

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium (BE)</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>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +32 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +32 78</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Bulgaria

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgaria (BG)</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></td>
<td>Toll-free prefixes: +359 800</td>
<td>Yes</td>
<td>Your name and address.</td>
</tr>
</tbody>
</table>

### Croatia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Croatia (HR)</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>Country Summary</td>
<td>Numbers Summary</td>
<td>ID Requirements</td>
<td>Acceptable Identification</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: + 385 95</td>
<td>Yes</td>
<td>Your business name, address, and business registration or VAT number.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: + 385 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Cyprus**

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyprus (CY)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: + 357 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Czech Republic**

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Czech Republic (CZ)</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></td>
<td>Mobile prefixes: +420 73</td>
<td>Yes</td>
<td>Your business name, address, and business registration or VAT number, and a copy of the ID or passport of an authorized representative.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +420 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Denmark**

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark (DK)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your name, address, and business registration or VAT number.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +45 25, +45 92, +45 41</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +45 808</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Estonia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonia (EE)</td>
<td>Toll-free prefixes: +372 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +372</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Finland

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland (FI)</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></td>
<td>Toll-free prefixes: +358 800</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +358 75</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### France

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>France (FR)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone. You must provide proof of the address along with a copy of the business registration.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +33 7</td>
<td>Yes</td>
<td>Your business name, address, and business registration or VAT number, and a copy of the ID or passport of an authorized representative. A global address and ID are acceptable.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +33 805</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +339</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Georgia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia (GE)</td>
<td>National prefixes: +995 70</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Germany

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany (DE)</td>
<td>Local telephone numbers: Yes</td>
<td>Yes</td>
<td>Your local address in the city corresponding to the geographical zone of requested number.</td>
</tr>
</tbody>
</table>

|                        | Toll-free prefixes: +49 800 | Yes | Your residence or business address outside of Germany. You must provide proof of the address. For numbers to be answered inside of Germany, a special process applies. You must obtain the number directly from the local regulator and then port it to Amazon Connect. Details about the process are provided when you make the request. |

|                        | National prefixes: +49 32 | Yes | Proof of your business address in Germany. |

Greece

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greece (GR)</td>
<td>Local telephone numbers: Yes</td>
<td>Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
</tr>
</tbody>
</table>

|                        | Toll-free prefixes: +30 800 | No |                           |


## Hong Kong

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong (HK)</td>
<td>National prefixes: +852 58</td>
<td>Yes</td>
<td>Your address and proof of address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A global address is acceptable.</td>
</tr>
</tbody>
</table>

## Hungary

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hungary (HU)</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: +36 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

## Indonesia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indonesia (ID)</td>
<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>
</tbody>
</table>

## Ireland

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ireland (IE)</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: +353 1800</td>
<td>No</td>
<td>Nomadic numbers (076) are distributed only to Irish</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +353 76</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Country Summary</td>
<td>Numbers Summary</td>
<td>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>residents, or to individuals with a proven, substantive association with Ireland.</td>
</tr>
<tr>
<td>Italy (IT)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Your business name, address, and VAT number. 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. Any Italian address is acceptable.</td>
</tr>
<tr>
<td>Mobile prefixes: +39 3</td>
<td>Yes</td>
<td>Your business name, address, and VAT number. 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. Any global address is acceptable.</td>
<td></td>
</tr>
<tr>
<td>Toll-free prefixes: +39 800</td>
<td>Yes</td>
<td>Your business name, address, and VAT number. 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</td>
<td></td>
</tr>
</tbody>
</table>
### Region requirements for phone numbers

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan (JP)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Businesses must provide a copy of the ID or passport of an authorized representative, a ZIP file containing a proof of address, and a document that associates the authorized representative with the business. 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); or IDs listing the submitted address, such as government-issued IDs, passports, drivers licenses, and business registration. The business address must be in the city corresponding to the requested area code of the number.</td>
</tr>
</tbody>
</table>

Toll-free prefixes: +81 120, +81 800 | Yes | Businesses must provide a copy of the ID or passport of an authorized representative, a ZIP file containing a proof of address, and a document that associates the authorized representative with the business. 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); or IDs listing the submitted address, such as government-issued IDs, passports, drivers licenses, and business registration. The business address must be in the city corresponding to the requested area code of the number. |
### Latvia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latvia (LV)</td>
<td>Mobile prefixes: +371 28</td>
<td>Yes</td>
<td>Your address. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +371 80</td>
<td>Yes</td>
<td>Your name and address. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +371 6</td>
<td>Yes</td>
<td>Your name and an address in Latvia.</td>
</tr>
</tbody>
</table>

### Lithuania

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lithuania (LT)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +370 66</td>
<td>Yes</td>
<td>Your business name, address and registration number. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +370 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Luxembourg

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Luxembourg (LU)</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></td>
<td>Toll-free prefixes: +352 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Malaysia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malaysia (MY)</td>
<td>Local telephone numbers: +60 15</td>
<td>No</td>
<td>Numbers can not be issued to businesses registered in Malaysia.</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +60 15</td>
<td>Numbers may not be issued to businesses registered in Malaysia.</td>
<td></td>
</tr>
</tbody>
</table>

### Malta

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malta (MT)</td>
<td>National prefixes: +356</td>
<td>Yes</td>
<td>Your business name, address, a copy of the business registration (global), and a copy of the ID or passport of an authorized representative. A global address is acceptable.</td>
</tr>
</tbody>
</table>

### New Zealand

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand (NZ)</td>
<td>Local telephone numbers:</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +64 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Netherlands

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands (NL)</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: +31 97</td>
<td>Yes</td>
<td>A global business address. No voice services are supported, only SMS.</td>
</tr>
</tbody>
</table>
|                 | Toll-free prefixes: +31 800 | Yes             | File orders in writing. 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.  
Estimated lead time from order to activation is 6 weeks. |
| National prefixes: +31 85 | No                   |                 |                                                                                         |

### Norway

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Norway (NO)</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>
|                 | Mobile prefixes: +47 59 | Yes             | Your business name, address, and registration number, and a copy of the ID or passport of an authorized representative.  
A global address is acceptable. |
|                 | Toll-free prefixes: +47 800 | Yes             | Your business address in Norway.                                                        |
|                 | National prefixes: +47 81 | Yes             | Your business address in Norway.                                                        |
## Poland

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland (PL)</td>
<td>Local telephone numbers: No</td>
<td></td>
<td>Your business name, address and registration number, and a copy of the ID or passport of an authorized representative. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +48 73 Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +48 800 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Portugal

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portugal (PT)</td>
<td>Local telephone numbers: Yes</td>
<td></td>
<td>Your business address. It must be in the relevant geographic zone. You must also submit the required proof of telecom services being provided to the address.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +35 1800 No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +351 30 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Romania

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Romania (RO)</td>
<td>Local telephone numbers: Yes</td>
<td></td>
<td>Your address and proof of address. It must be in the relevant geographic zone.</td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +40 800 No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +40 376 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Singapore

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore (SG)</td>
<td>Mobile prefixes: +65 8</td>
<td>Yes</td>
<td>Proof of the business address and registration number, and the country of incorporation. A global address is acceptable.</td>
</tr>
<tr>
<td></td>
<td>National prefixes: +65 31</td>
<td>Yes</td>
<td>Proof of the business address and registration number, and the country of incorporation. A global address is acceptable.</td>
</tr>
</tbody>
</table>

## Slovakia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slovakia (SK)</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: +421 800</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

## Slovenia

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slovenia (SI)</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>No</td>
<td></td>
</tr>
</tbody>
</table>
## Spain

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spain (ES)</td>
<td>Local telephone numbers: Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +34 900 No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +34 518, +34 902 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Sweden

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden (SW)</td>
<td>Local telephone numbers: Yes</td>
<td>Your business address in Sweden.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile prefixes: +46 766 No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +46 20 No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>National prefixes: +46 77 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Switzerland

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switzerland (CH)</td>
<td>Local telephone numbers: Yes</td>
<td>Your business address. It must be in the relevant geographic zone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-free prefixes: +41 800 No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Thailand

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thailand (TH)</td>
<td>Local telephone numbers: Yes</td>
<td>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>
</tbody>
</table>
### Set up routing

In Amazon Connect, routing consists of three parts: queues, routing profiles, and contact flows. This topic discusses queues and routing profiles. For information about contact flows, see Create Amazon Connect contact flows (p. 152).

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.

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>The address cannot be in Thailand.</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 of an authorized representative. The address cannot be in Thailand.</td>
<td></td>
</tr>
</tbody>
</table>

**Turkey**

<table>
<thead>
<tr>
<th>Country Summary</th>
<th>Numbers Summary</th>
<th>ID Requirements</th>
<th>Acceptable Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turkey (TR)</td>
<td>Local telephone numbers:</td>
<td>Yes</td>
<td>Proof of business address. It must be in the city corresponding to the requested area code. The business registration and a copy of the ID or passport of an authorized representative.</td>
</tr>
<tr>
<td>Toll-free prefixes: +90 800</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>National prefixes: +90 850</td>
<td>Yes</td>
<td>Your business address and a copy of the ID or passport of an authorized representative. A global address is acceptable.</td>
<td></td>
</tr>
</tbody>
</table>

**United States**

There aren't any documentation requirements for international customers to claim phone numbers in the United States.
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): voice, chat, or both.
- How many chat conversations agents can handle simultaneously, up to 5.
- Whether individual queues are for voice, chat, or both.

Each agent is assigned to one routing profile.

Contents
- How routing works (p. 119)
- Create a queue (p. 120)
- Disable a queue (p. 120)
- Set the Maximum contacts in queue limit (p. 121)
- Set the hours of operation and timezone for a queue (p. 122)
- Set up outbound caller ID (p. 124)
- Create a routing profile (p. 126)
- Set up queue-based (skills-based) routing (p. 128)

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 contact 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 contact 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.
- 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 available, the contact is routed to the agent who has been in the Available status for the longest time.
- 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 both voice and chat channels, agents must complete the interactions with inbound contacts on one channel before they can receive a contact on the other.

Example: Say a routing profile is configured for voice contacts and for up to 5 chats. Here’s how it would work:
Create a queue

1. Choose Routing, Queues, Add new queue.
2. Add the appropriate information about your queue and choose Add new queue.
   
   The queue is automatically active.
3. Assign the queue to a routing profile; for information, see Create a routing profile (p. 126). The routing profile links the queue and agents together.

To learn how queues work, see Routing profiles (p. 14) and Queue-based routing (p. 19).

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. 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.

Set the Maximum contacts in queue limit

You can define routing decisions based on queue capacity. For example, use a Transfer to queue block to check whether a queue is full, and then route the contact accordingly.

The Transfer to queue block checks the maximum capacity limit you set here. If no limit is set, the queue is limited to the number of concurrent contacts set in the service quota for the instance.
1. Choose **Routing, Queues, Add new queue**. Or, edit an existing queue.
2. Under **Maximum contacts in queue** choose **Set limit**.
3. Specify how many contacts can be in the queue before it's considered full.

### 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 contact 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.

**To set the hours of operation and timezone for a queue**

1. 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**

<table>
<thead>
<tr>
<th>Day</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Monday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Tuesday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Wednesday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Thursday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Friday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
<tr>
<td>Saturday</td>
<td>12:00 AM</td>
<td>12:00 AM</td>
</tr>
</tbody>
</table>

**Schedule for Monday to Friday 9:00 AM to 5:00 PM**

Remove Sunday and Saturday from the schedule.
Set the hours of operation

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 (p. 130) 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 (p. 130)
- About agent status (p. 414)
- Change the "Agent activity" status in a real-time metrics report (p. 438)
What happens during daylight savings time

Amazon Connect uses the timezone to determine whether daylight savings time is in effect for the queues, and adjusts automatically. 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.

Use the Check Hours of Operation block

At the start of your contact flows, use the Check hours of operation (p. 210) block to determine whether your contact center is open, and to branch accordingly.

Set up outbound caller ID

We recommend setting your outbound caller ID. Not doing so may result in some PSTN carriers considering your outbound calls fraudulent activity, and they may drop them.

There are a few times when your outbound caller ID—your company name and number—will appear to contacts:

- During customer callbacks.
- If an agent makes an outbound call.
- If an agent transfers a call, for example, to an external number.

There are a few places where you can specify what your outbound caller ID:

- In a queue. You can specify both the outbound caller ID name and the phone number. For instructions, see Create a queue (p. 120).
- In the Call phone number block in an outbound whisper contact flow. You can 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.
- In the Transfer to phone number (p. 267) block.

Use the Call phone number block to set caller ID

Use the Call phone number (p. 203) 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 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 the block to display a phone number for a specific line of business, or for displaying different numbers to customers based on their account type.

There are two ways you can set up how caller ID works for outbound calls:

- Select any phone number from your instance.
- Or, use an attribute to set the number dynamically during the contact flow.

Only phone numbers that you've claimed (p. 95) or ported to Amazon Connect (p. 97) can be used as your caller ID number.

About using dynamic caller ID

If you use an attribute to set the caller ID number dynamically, the attribute can be one you define in the Set contact attributes block in the contact 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.

### 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.

Phone numbers that are not formatted in E.164 may work, but it depends on the phone or handset that is being used as well as the carrier from which the call is originated.

When you place calls from the CCP using Amazon Connect the CCP provides the correct formatting for numbers automatically.

### How caller ID works in Call phone number block

Outbound whisper flows execute in Amazon Connect immediately after an agent accepts the call during direct dial and callback scenarios. When the contact flow executes:

- 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 ACW status.

The Call phone number block is supported only in outbound whisper flow contact flows. Only published contact flows can be selected as the outbound whisper flow for a queue.

### Specify a custom caller ID number using a Call phone number block

1. In Amazon Connect choose Routing, Contact flows.
2. Choose the down arrow next to Create contact 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 contact 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.

6. Add any additional blocks to complete your contact flow, and connect the **Success** branch of the **Call phone number** block to the next block in the flow. Note that there is no error branch for the block. If a call is not successfully initiated, the contact flow ends and the agent is placed in an **AfterContactWork** (ACW) state.

**Why your caller ID might not appear correctly to customers**

Amazon Connect presents Outbound Caller ID Name correctly via the Calling Line/Party Presentation service on outbound calls. In testing, with all of our telephony providers, the Outbound Caller ID Name value comes back to us intact on all the carriers we use. This service is not consistent because downstream carriers (including mobile carriers) often ignore the value we set in the Outbound Caller ID Name and CNAM is not regulated or enforced.

**How to avoid labels like "spam" and "telemarketer"**

Amazon Connect has contracted with a leading provider of CNAM services for US numbers to provide Calling Name to the extent possible. This enables outbound calls that show the enrolled Calling Line Identity (CLI) to generally avoid reputation-sensitive labels like "spam" or "telemarketer."

To enroll your numbers with this CNAM services provider, open a Support ticket. Our Support team will gather the required information to enroll your numbers. For instructions on how to access Support, see **Get administrative support for Amazon Connect (p. 593).**

**Note**

Only numbers in the 50 US states, Puerto Rico, and Virgin Islands are eligible.

**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 which queues will be in it. You can also specify whether one queue should be prioritized over another.

Each agent is assigned to one routing profile.

**To create a routing profile**

1. Choose **Users, Routing profiles, Add new profile.**
2. Enter or choose the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a searchable display name.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe what the routing profile is for.</td>
</tr>
<tr>
<td>Set channels and concurrency</td>
<td>Choose whether agents assigned to this profile handle contacts using voice, chat, or both.</td>
</tr>
</tbody>
</table>
### Create a routing profile

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For Chat,</strong> specify up to five chat conversations that an agent can have simultaneously. For more on setting this option, see Tips for setting up channels and concurrency (p. 128). For information about how Amazon Connect routes contacts when multiple channels are in use, see How routing works with multiple channels (p. 119).</td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Use the dropdown menu to choose a queue you've already set up. You can add multiple queues to a routing profile.</td>
</tr>
<tr>
<td><strong>Channels</strong></td>
<td>Choose whether the queue is for chat, voice, or both. <strong>Important</strong> The channel that you specify here must also be specified under Set channels and concurrency. 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><strong>Delay (in seconds)</strong></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 Queues: priority and delay (p. 17).</td>
</tr>
</tbody>
</table>

3. **Under Routing profile queues,** enter the following information:
### Set up queue-based routing

Here's an overview of the steps to set up queue-based routing:

- **Create the queues (p. 120),** for example, one for each skill you want to use for routing.
- **Create the routing profiles (p. 126):**
  - Specify the channels supported by this routing profile.
  - Specify the queues: the channel, priority, and delay.
- **Configure agent settings (p. 131) to assign the routing profiles to them.**

When you **create your contact flows (p. 169),** 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 (p. 119)
- Queue-based routing (p. 19)

### 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.
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 (p. 468).

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.

Create a new agent hierarchy

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.

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 (p. 438) 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 and drag it to the order you want.
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)?
- 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 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. In the navigation pane, go to Users, User management.
2. Choose the user you want to configure, then choose Edit.
3. Assign a routing profile (p. 126) 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.
Enable auto-accept call

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.

Auto-Accept Call doesn’t work for callbacks.

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. You can also configure the setting for multiple new users when you bulk upload new users with the CSV template.

Enable auto-accept call for existing agents

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 your Amazon Connect instance using your access URL (https://domain.awsapps.com/connect/login).
2. In the left navigation bar, 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. In the left navigation bar, 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
```

Log out agents automatically when they close their CCP

When using the default Amazon Connect CCP, closing the CCP window doesn't change an agent's status from Available to Offline. An agent must change their status manually, and then log out.

To change this behavior, you must create a custom CCP.

Use the Amazon Connect Streams API and the Agent API to create a custom CCP for your contact center. For an example custom CCP setup, see Perform an external screen pop with Amazon Connect.

Use the following steps to update your CCP so it 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.

```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 contact 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.

Upgrade to the latest CCP

The URL for the latest Contact Control Panel (CCP) looks like this: https://name of your instance. awsapps.com/connect/ccp-v2/

You only need to upgrade to the latest CCP if you're using one the following options:

- The URL for your CCP ends with `/ccp#` (p. 135)
• You use the Amazon Connect Streams API (p. 146). 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 (p. 136) 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#` (p. 135)
• I use the Amazon Connect Streams API (p. 146)

**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 (p. 136).
• 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.
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 allow list (p. 321).

Using this option helps Amazon Connect Support to quickly troubleshoot any issues you have. Specifically, using `*.execute-api.{region}.amazonaws.com` passes more metrics to our Support team to help with troubleshooting.

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.
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**

![Earlier CCP](image1)

![Latest CCP](image2)
Miss a call

Earlier CCP

Latest CCP

Make a call: When to use Quick connects

Earlier CCP

Latest CCP

- 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
My CCP URL ends with /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

Latest CCP

Miss a queued callback

Earlier CCP

Latest CCP
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:
   2. Navigate to the Amazon Connect console.
   3. Check that you're in the correct Region for your Amazon Connect instance. Choose your instance.
4. Choose **Application integration**, and then choose **Add origin**.

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 allow list to prevent any issues with the CTI Adapter CCP functionality. For detailed instructions, see Amazon Connect CTI Adapter v5 for Salesforce Lightning installation guide or the Amazon Connect CTI Adapter v5 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 allow list (p. 321).

Using this option helps Amazon Connect Support to quickly troubleshoot any issues you have. Specifically, using `*.execute-api.{region}.amazonaws.com` passes more metrics to our Support team to help with troubleshooting.
Provide access to the Contact Control Panel

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. **Add agents** (p. 357) to your instance. This creates a user name and password for them to log into the CCP.
2. **Assign them the "Agent" security profile** (p. 364). This grants them permissions to access the CCP.
3. Give them their user name, password, and a link to the CCP so they can log in. The CCP is a website. The URL to your CCP is:
   
   • [https://name of your instance.awsapps.com/connect/ccp-v2/](https://name of your instance.awsapps.com/connect/ccp-v2/)

   We recommend telling agents to bookmark the URL to the CCP so they can access it easily.
4. **Train your agents on the CCP:**
   
   • Watch Training video: How to use the CCP (p. 537)
   • Download a quick start cheat sheet.

Grant microphone access in Chrome or Firefox

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

Microsoft Edge is not a supported browser for accessing the Contact Control Panel.

**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 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)* (p. 560) 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.

**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**—The latest three versions of Google Chrome or Mozilla Firefox
- **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 and Contact Control Panel (CCP) do not work on 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://yourInstanceName.awsapps.com), and also your signaling address for endpoints.
- Regular monitoring of workstations that show processes running, and the current resource usage of each process.
- Workstation performance/utilization in these areas:
  - Processor (CPU)
Can't hear caller or caller can't hear agent?

When the agent can't hear the caller or the caller can't hear them, it's usually because there are problems with one of the following:

- 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, following the steps under **Downloading Streams**. You can also resolve the issue by using Firefox as your browser.

For more information about solving audio problems, see **Troubleshooting Issues with the Contact Control Panel (CCP)** (p. 560).

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 allow list in the agent's Chrome settings. For instructions, see this **Google Chrome Help article**.
For more information about solving audio problems, see Troubleshooting Issues with the Contact Control Panel (CCP) (p. 560).
Create Amazon Connect contact flows

A contact flow defines the customer experience with your contact center from start to finish. Amazon Connect includes a set of default contact flows (p. 152) so you can quickly set up and run a contact center. However, you may want to create custom contact flows for your specific scenario.

Default contact flows

Amazon Connect includes a set of default contact flows that have already been published. It uses them to power your contact center.

For example, say you create a contact flow that includes putting the customer on hold, but you don’t create a prompt for it. The default contact 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 contact flow, we recommend creating a new customized flow based on the default. Then call the new flow intentionally in your contact flows rather than defaulting to it. This gives you better control over how your contact flows work.

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

Change how a default contact 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.

1. On the navigation menu, choose Routing, Contact flows.
2. Choose the default contact 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.
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, as shown in the following image.

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 contact flow before customizing it

Use the following steps to create a new flow based a current default.

1. On the navigation menu, choose Routing, Contact flows.
2. Choose the default contact flow you want to customize.
3. In the upper right corner of the page, choose the Save drop-down arrow. Choose Save as.
4. Assign a new name for the contact flow, for example, Customer hold message.
5. Add the new contact flow (in this case, Customer hold message) to the contact 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.

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 153).

**Default agent transfer: "Transferring now"**

This default transfer flow is the what the agent experiences when transferring a contact to another agent by using Create quick connects (p. 179). A **Play prompt** plays the message “Transferring now.” Then the **Transfer to agent** block is used to transfer the contact to the agent.

**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 (p. 189).

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 153).

**Default customer queue: queue hold message and music**

This default contact 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, Contact flows.
2. Choose Default customer queue.

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, as shown in the following image.
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 contact flow uses a Set whisper flow (p. 253) 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 (p. 253) block to override the default agent whisper in a voice conversation.

**Important**
For chat conversations, you need to include a Set whisper flow (p. 253) for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation (p. 159).

Default agent whisper: name of the queue

This contact flow uses a Set whisper flow (p. 253) 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 (p. 253) block to override the default agent whisper in a voice conversation.

**Important**
For chat conversations, you need to include a Set whisper flow (p. 253) for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation (p. 159).

For more information about system variables, see Contact flow system attributes (p. 289).

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 (p. 162):

1. Go to Routing, Contact 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:

![Sample inbound flow (first contact experience)](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.

4. Choose Save.

**Default customer hold: hold music**

This contact 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 contact flow, see Change a default contact flow (p. 153).

**Default outbound: "This call is not being recorded"**

This contact 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 contact flow, see Change a default contact flow (p. 153).
Default queue transfer: "Now transferring"

This contact 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 contact flow, see Change a default contact flow (p. 153).

**Default prompts from Amazon Lex: "Sorry .. "**

If you add an Amazon Lex bot 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 contact flows

Amazon Connect includes a set of sample contact flows that show you how to perform common functions. They are designed to help you learn how to create your own contact 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** (p. 167) flow.

**To explore how the sample flows work**

1. Claim a number if you haven't already: go to Routing, Phone numbers, Claim a number.
2. Choose the **DID** tab, then choose a number.
3. In **Contact flow / IVR** use the drop down to choose the sample contact flow you want to try. Click Save.
4. Call the number. The sample contact flow that you selected starts.

   We recommend opening the sample contact flow in the contact flow designer and following along to see how it works while you're experiencing it.

**To open a sample flow in the contact flow designer**

1. In Amazon Connect choose **Routing, Contact flows**.
2. On the **Contact 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 contact flows work.

Contents

- Sample inbound flow (first contact experience) (p. 162)
- Sample AB test (p. 162)
- Sample customer queue priority (p. 163)
- Sample disconnect flow (p. 163)
- Sample queue configurations (p. 163)
- Sample queue customer (p. 166)
- Sample queued callback (p. 167)
- Sample interruptible queue flow with callback (p. 167)
- Sample Lambda integration (p. 168)
- Sample recording behavior (p. 168)
- Sample note for screenpop (p. 168)
- Sample secure input with agent (p. 169)
- Sample secure input with no agent (p. 169)

Sample inbound flow (first contact experience)

Type: Contact flow (inbound)

This sample flow is automatically assigned to the phone number that you claimed when you first set up contact flows. For more information, see Get started (p. 7).

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 Set disconnect flow.
- If the channel is voice, the customer is transferred to the other sample contact flows, based on their input.

Sample AB test

Type: Contact flow (inbound)

This contact 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 (p. 162).
Sample customer queue priority

Type: Contact flow (inbound)

Note
This sample flow is available in previous Amazon Connect instances. In new instances, you can see this functionality in Sample queue configurations (p. 163).

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

Type: Contact flow (inbound)

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.

Sample queue configurations

Type: Contact flow (inbound)

This contact 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.

   You can see this path in the following image:

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 (p. 270)** block to put the customer in a callback queue.

6. The **Transfer to queue (p. 270)** 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 (p. 191)
- Contact block: Transfer to queue (p. 270)
- About queued callbacks in metrics (p. 417)

Sample queue customer

Type: Contact flow (inbound)

This contact 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**

Type: Contact flow (inbound)

**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** (p. 167) and **Sample queue configurations** (p. 163).

This contact 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** (p. 191)
- **Contact block: Transfer to queue** (p. 270)
- **About queued callbacks in metrics** (p. 417)

**Sample interruptible queue flow with callback**

Type: Customer queue

This contact 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

Type: Contact flow (inbound)

This contact 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 or chat. 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 Using attributes with a Lambda function (p. 279).

Sample recording behavior

Type: Contact flow (inbound)

This contact flow starts by checking the channel of the customer:

- 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 (p. 162).

For more information, see the following topics:

- Set up recording behavior (p. 190)
- Monitor live conversations (p. 367)
- Review recorded conversations (p. 370)

Sample note for screenpop

Type: Contact flow (inbound)

This contact 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**

Type: Queue transfer

This contact 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 (p. 344) 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**

Type: Contact flow (inbound)

This contact 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 (p. 162).
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 .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 (p. 162).

**Create a new contact flow**

The starting point for creating all contact flows is the contact 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 action blocks, see Contact block definitions (p. 201).
Before you begin: develop a naming convention

Chances are you’re going to create tens or hundreds of contact flows. To help you stay organized, it’s important to develop a naming convention. Once you start creating contact flows, we strongly recommend against renaming them.

You can’t delete a contact flow. To get obsolete contact flows out of your way, we recommend appending `zzTrash_` to their name. This will also make them easy to find should you want to reuse them in the future.

Choose a contact flow type

Amazon Connect includes a set of nine contact flow types. Each type has only those blocks for a specific scenario. For example, the contact flow type for transferring to a queue contains only the appropriate contact blocks for that type of flow.

**Important**

- When you create a contact 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 contact flow types are available.

<table>
<thead>
<tr>
<th>Type</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound contact flow</td>
<td>This is the generic contact flow type that’s created when you choose the Create contact flow button, and don’t select a type using the drop-down arrow. It creates an inbound contact flow. This contact flow works with voice and chat.</td>
</tr>
<tr>
<td>Customer queue flow</td>
<td>Use to manage what the customer experiences while in queue, before being joined to an agent. Customer queue flows are interruptible and can include actions such as an audio clip apologizing for a delay and offering an option to receive a callback, leveraging the Transfer to queue block. This contact flow works with voice and chat.</td>
</tr>
<tr>
<td>Customer hold flow</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. This contact flow works with voice.</td>
</tr>
<tr>
<td>Customer whisper flow</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>
</tbody>
</table>
## Create an inbound contact flow

Use these steps to create an inbound contact flow.

1. In the navigation pane, choose **Routing**, **Contact flows**.
2. Choose **Create contact flow**. This opens the contact flow designer and creates an inbound contact flow (Type = Contact flow).
3. Type a name and a description for your contact flow.
4. Search for a contact block using the **Search** bar, or expand the relevant group to locate the block. For descriptions of the contact blocks, see **Contact block definitions** (p. 201).

### Type | When to use
--- | ---
This contact flow works with voice.
**Outbound whisper flow** | 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.
This contact flow works with voice.
**Agent hold flow** | 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 contact flow works with voice.
**Agent whisper flow** | 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.
**Transfer to agent flow** | 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 **Transfer to agent** block.
This contact flow works with voice.
**Transfer to queue flow** | 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 **Transfer to queue** block.
This contact flow works with voice and chat.
5. Drag and drop contract blocks onto the canvas. You can add blocks in any order or sequence, as connections between elements aren't required to be strictly linear.

    **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 contact 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 contact 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 contact flow.

### Generate logs

After your contact flow is published live, you can use contact flow logs to help analyze contact flows and quickly find errors your customers encounter. If needed, you can roll back to a previous version of the contact flow.

For more information about using contact flow logs, see [Track events as customers interact with contact flows](p. 198).

### Copy and paste contact 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 contact blocks.
- The layout arrangements.
- The connections.

**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. 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.
Roll back a contact flow

1. In the contact flow designer, open the contact flow you want to roll back.
2. Use the drop-down to choose the version of the contact 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.

   **Note**
   To see a consolidated view of all changes across all flows, click the [View historical changes](#) link at the bottom of the Contact flows page. You can filter to a specific flow by date or user name.

3. Choose **Publish** to push that version into production.

Associate a phone number with a contact flow

After you publish a contact flow, you can associate a phone number with it.

**To associate a phone number with a contact flow**

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose **Routing, Phone numbers**.
3. You can search for a specific number, filter your search by queue, or select a number from the list provided (if applicable).
4. Click on the number to edit it.
5. Expand **Contact flow / IVR**, and select the contact flow to associate with the phone number. Only published contact flows are listed.
6. Choose **Save**. When a contact calls the number, they are connected to that contact flow.

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 contact flows. Or, you can add your own recordings.

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 due to PSTN limitations (here's a Wikipedia article that provides details: G.711). This may result in low quality audio.

We recommend that you align your prompts and routing policies with each other to ensure a smooth call flow for customers.

To create a prompt

1. In the navigation pane, choose Routing, Prompts.
2. On the Manage voice prompts page, choose Create new prompt.
3. Choose the following actions:
   - Upload—Select the file to upload.
   - Record—Select the red circle to begin recording. Use the red square to stop. You can choose Crop to cut the recorded prompt or Discard to record a new prompt.
4. For Step 2: Input basic information, enter the name of the file, and then choose Create.

Maximum length for prompts

Amazon Connect supports prompts that are less than 50 MB and less than 5 minutes long.

Bulk upload of prompts

Currently bulk upload of prompts is not supported through the Amazon Connect console or programmatically.

Add text-to-speech to prompts

You can enter text-to-speech prompts in the following contact flow blocks:

- Get customer input (p. 218)
- Loop prompts (p. 234)
- Play prompt (p. 236)
- Store customer input (p. 261)

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 are free. You are charged only for using custom 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 contact 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/.
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 Contact flows.
5. In the Amazon Polly section, choose Use the best available voice.

How to add text-to-speech

1. In a contact flow, add the block that will play the prompt. For example, add a Play prompt (p. 236) block.
2. In the Properties, choose Text-to-speech.
3. Enter plain text, as shown in the following image.
Choose the voice for audio prompts

Or enter SSML:

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 (p. 178).

For more information about Amazon Polly, see Using SSML in the Amazon Polly Developer Guide.

Choose the voice for audio prompts

You select the text-to-speech voice and language in the Set voice (p. 251) 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 contact 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 contact flow block for interpreting text-to-speech is Text. To use SSML for text to speech in your contact 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. To learn more about the SSML tags, see Supported SSML Tags in the Amazon Polly Developer Guide.

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 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 SSML Tags Supported by Amazon Polly.

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

To make it easy for you to set up contact transfers, Amazon Connect provides you with several tools:
Two contact flow types:
- Transfer to agent: Enables transfers to another agent. This works with voice contacts.
- Transfer to queue: Enables transfers to a queue. This works with both voice and chat contacts.

Contact blocks:
- Transfer to queue (p. 270): Use to end the current contact flow and place the customer in a queue. This block works for both voice and chat transfers.
- Transfer to phone number (p. 267): Use to transfer the customer to a phone number, such as an external number. This block works for voice transfers.
- Transfer to flow (p. 265): Use to end the current flow and transfer the customer to another contact flow. This block works for voice transfers.
- Quick connects: Use to create common destinations for transfers. Agents will see them as options in the CCP when they go to do a transfer.

This topic explains how to create quick connects and use transfer contact blocks in specific scenarios.

Overview of steps

To set up call transfers and quick connects
1. Choose a contact flow type based on what you want to do: Transfer to agent or Transfer to queue. External transfers do not require a specific type of contact flow.
2. Create and publish the contact flow.
3. Create a quick connect for the type of transfer to enable: Agent, Queue, or External.
   When you create the Agent or Queue quick connect, select a contact flow that matches the type of transfer to enable. External quick connects require only a phone number, and do not allow you to set a queue or contact flow.
4. Add the quick connect that you created to any queue used in a contact flow for which to enable contact transfer, such as the queue used in the contact 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.

Types of quick connects

The type of a quick connect specifies the destination. You can specify one of the following destinations.

External quick connect

Contacts are transferred to an external number (such as an on-call pager).

Agent quick connect

Contacts are transferred to a specific agent as part of a contact flow.

If you want all of your agents to appear individually in the list of quick connects in the Contact Control Panel (CCP), you need to add each one manually. There's no way to automate this process.
Important
Agent 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 contact flow.

Important
Agent and Queue quick connects only appear in the CCP when an agent goes to transfer a contact.

Step 1: Create quick connects

To create a quick connect

1. 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), contact 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.

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 all of the quick connects for the queues in their routing profile.

Delete quick connects

At this time you can't delete quick connects. You can reuse them by changing the type, destination, and contact flow on the Quick connects page.

Or, you can remove them from a queue on the Edit queue page so that agents can't see them in the Contact Control Panel (CCP).
How quick connects work

This article explains how each type of quick connect works: agent, queue, and external quick connects. It explains which contact 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 (p. 160) flow unless you specify a different customer hold flow.

Agent 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 an agent quick connect.

Here's what John and Maria do, and what contact 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:
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** (p. 253) 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** (p. 159), which says the queue name.

7. The next **Set whisper flow** (p. 253) 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** (p. 159), 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 contact 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 (p. 270) 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 (p. 170) is played to Maria. It says "Connecting you to PasswordReset queue."

6. The Customer whisper flow (p. 170) 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.

**External quick connects**

There are no contact flows involved in external quick connect. When an agent invokes an external quick connect, the call is directly connected the destination without invoking any flows.

Because no contact flow is involved in external quick connects, you can't set the outbound caller ID. Instead, the caller ID that you specified when you created the queue (p. 120) is used.

**Set up agent-to-agent transfers**

We recommend using these instructions to set up agent-to-agent voice and chat transfers. You use a Set working queue (p. 256) 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) (p. 264) block does not.

**Step 1: Create the quick connect**

**Create a quick connect**

1. 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), contact 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" contact flow

In this step, you create a contact flow that's type Transfer to agent and use a Set working queue (p. 256) block to transfer the contact to the agent.

1. In the navigation pane, choose Routing, Contact flows.
2. Use the drop-down to choose Create transfer to agent flow.
3. Type a name and a description for your contact 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:
1. Choose **By agent**.
2. Choose **Use attribute**.
3. For **Type**, use the dropdown box to select **Agent**.
4. For **Attribute**, use the dropdown box to select **User name**.
6. Add a **Transfer to queue (p. 270)** block. You don't need to configure this block.
7. Save and publish this contact flow.

8. To show your agents how to transfer chats to another agent, see Transfer chats to another queue (p. 545).

Resume a contact 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 external number, you want them to be returned to your agent, for example, when the delivery company couldn’t resolve their issue.

- For advanced automation, 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 contact 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.
     - **Use attribute**—Specify a contact attribute 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.
     - **Use attribute**—Specify a contact attribute to use to set the Timeout duration.

   - **Resume contact flow after disconnect**—When you select this option, after the call is transferred, the caller is returned to the contact 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.
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 contact 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 How to use system metric attributes (p. 284).

After determining which queue to transfer the contact to, use a **Transfer to queue** block in a contact 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 (p. 121) 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 (p. 566) 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, choose **Routing, Contact flows**.
2. Choose the down arrow next to **Create contact 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 **Use attribute**, 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 contact flow that you require, such as the blocks to check queue status or metrics, then choose **Save**.
   The contact 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 contact 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 contact flow designer, open an existing contact 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 contact 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 contact 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 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.

You can also find the user ID for an agent by using Amazon Connect agent event streams (p. 474). 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"
        }]
      }
    }
  }
```
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 (p. 249) block to your contact 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?**

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 a customer is on hold, the agent is still recorded.

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 (p. 87). 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 contact flow block using the Set recording and analytics behavior (p. 249) 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 (p. 249) block to the flow.

**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 (p. 370).
Important
You can also access the recording from the customer's contact trace record (CTR) (p. 469). The recording is available in the CTR, however, only after the contact has left the After Contact Work (ACW) state (p. 414).

How to set up recording behavior
To view a sample contact flow with the Set recording behavior block configured, see Sample recording behavior (p. 168).

To set up recording behavior in your contact flows
1. Log in to your Amazon Connect instance using an account that has permissions to edit contact flows.
2. Choose Routing, Contact flows, and then open the contact flow that handles customer contacts you want to monitor.
3. Before the contact is connected to an agent, add a Set recording and analytics behavior (p. 249) block to the contact flow.
4. To configure the Set recording and analytics behavior (p. 249) 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.
5. Choose Save and then Publish to publish the updated contact flow.

To set up recording behavior for outbound calls
1. Create a contact flow, using the outbound whisper flow type.
2. Add a Set recording and analytics behavior (p. 249) 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 contact flow that has Set recording and analytics behavior (p. 249) 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:
   • Monitor live conversations (p. 367)
   • Review recorded conversations (p. 370)

Set up queued callback
You can create contact flows that provide the ability for customers to leave their phone number and get a callback from an agent.

Here's how queued callback works:
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 stay in queue for up to 7 days after they are created. After that, they are automatically removed from the queue.

3. If there is no answer when the Amazon Connect calls the customer, it retries based on the number of times you’ve specified. If the call goes to voicemail, it’s considered connected.

Steps to set up queued callback

Use the steps provided in the following overview to set up queued callback.

- **Set up a contact queue** (p. 120) 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** (p. 124). 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** (p. 126). Set this up so that contacts waiting for a call are routed to agents.
- **Create a contact flow for queued callbacks** (p. 192). You offer the option for a callback to the customer.
- **Associate a phone number with the inbound contact flow** (p. 173).
- (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..."

Create a contact flow for queued callbacks

To see what a flow looks like with queued callback, in new Amazon Connect instances see Sample queue configurations (p. 163). In previous instances, see Sample queued callback (p. 167).

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.
Following are the steps to create this flow.

**To create a contact flow for queued callbacks**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. Select an existing contact flow, or choose **Create contact flow** to create a new one.
   
   **Tip**

   You can create this flow using different contact flow types: Customer queue flow, Transfer to agent, Transfer to queue.

3. Add a **Get customer input (p. 218)** block.
4. Configure the block to prompt the customer for a callback:

   ![Get customer input block configuration](image)

5. At the bottom of the block, choose **Add another condition**, and add options 1 and 2.

6. Add a **Store customer input (p. 261)** block.
7. Configure the block to prompt customers for their callback number, such as “Please enter your phone number.”
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 contact flow.

10. Configure the block to set **Type** to **System**. For **Attribute**, choose **Store customer input**. This attribute stores the customer's phone number.
11. Add a **Transfer to queue (p. 270)** block.

12. In the **Transfer to queue** block, configure the **Transfer to callback queue** tab as shown in the following image:

   ![Image of Set callback number](image)

   **Set callback number**

   Specifies the number to be used to call the customer back in the Contact Control Panel (CCP), or when Transfer to queue is invoked with the callback option.

   **Use attribute**

   **Type**

   System

   **Attribute**

   Stored customer input

   **Initial delay**: Specify how much time has to pass between a callback contact being initiated in the contact 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.

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 (p. 163). For previous instances, see Sample queued callback (p. 167).

15. For information about how callbacks appear in real-time metrics reports and CTRs, see About queued callbacks in metrics (p. 417).

**Learn more about queued callbacks**

See the following topics to learn more about queued callbacks:

- About queued callbacks in metrics (p. 417)
- How Initial delay affects Scheduled and In queue metrics (p. 419)
- What counts as a "Failed Callback Attempt" (p. 420)
- Example: Metrics for a queued callback (p. 420)
Import/export contact flows

Use the procedures described in this topic to import/export a few contact flows from one instance to another, or from one Region to another as you expand your customer service organization.

To migrate tens or hundreds of contact flows, use the APIs described in Migrate contact flows to a different instance (p. 294).

**Note**
The Contact Flow Import/Export feature is currently in Beta status. Updates and improvements that we make could result in issues in future releases importing contact flows that are exported during the beta phase.

**Export limitations**

You can export contact 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 into smaller ones to meet these requirements.

**Contact flows are exported to JSON files**

A contact 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 contact flow may be different than the label used for it in the user interface (UI).

By default, contact 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 contact flows to a folder that contains only exported contact flows.

**How to import/export contact flows**

**To export a contact flow**

1. Log in to your Amazon Connect instance using an account that is assigned a security profile that includes view permissions for contact flows.
2. Choose **Routing, Contact flows**.
3. Open the contact flow to export.
4. Choose **Save, Export flow**.
5. Provide a name for the exported file, and choose **Export**.

**To import a contact flow**

1. Log in to your Amazon Connect instance. The account must be assigned a security profile that includes edit permissions for contact flows.
2. Choose **Routing, Contact flows**.
3. Do one of the following:
Resolve resources in imported contact flows

When you create a contact flow, the resources you include in the contact flow, such as queues and voice prompts, are referenced within the contact 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 contact flow, the name and ARN for each resource referenced in the contact flow is included in the exported contact flow.

When you import a contact flow, Amazon Connect attempts to resolve the references to the Amazon Connect resources used in the contact flow, such as queues, by using the ARN for the resource. When you import a contact flow into the same Amazon Connect instance that you exported it from, the resources used in the contact 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 contact 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 contact 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 contact 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 contact 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 contact flow with unresolved or missing resources, but you cannot publish it until the resources are resolved or removed.

Track events as customers interact with contact flows

Amazon Connect contact flow logs provide you with real-time details about events in your contact flows as customers interact with them. You can also use contact flow logs to help debug your contact flows as you are creating them. If needed, you can always roll back (p. 173) to a previous version of a contact flow.

Contents

- Contact flow logs stored in an Amazon CloudWatch log group (p. 199)
- Enable contact flow logs (p. 199)
- What data is gathered in contact flow logs (p. 200)
- Track customers between contact flows (p. 201)
- Create alerts for contact flow log events (p. 201)
Contact flow logs stored in an Amazon CloudWatch log group

Contact flow logs are stored in an Amazon CloudWatch log group, in the same region as your Amazon Connect instance. This log group is created automatically when Enable contact flow logging (p. 199) 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 contact flow is triggered. You can configure CloudWatch to send alerts when unexpected events occur during active contact 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 contact flow logging**

You are not charged for generating contact 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 contact flow logs**

**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.
2. Choose the instance alias for your instance.
3. Choose Contact flows.
4. Scroll to bottom of the page. Select Enable Contact flow logs and choose Apply.

**Step 2: Add the Set logging behavior block**

Logs are generated only for contact flows that include a Set logging behavior (p. 249) 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 contact flow logs for a contact flow**

1. Add a Set logging behavior (p. 249) 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 contact flow that is already published, you must publish it again to start generating logs for it.

**What data is gathered in contact flow logs**

Log entries for contact 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 contact 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 contact flow that interact with or capture sensitive data or customers’ personal information.

If you use Amazon Lex or AWS Lambda in your contact flows, the logs show the entry and exit of the contact 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 contact flow ID, and the contact flow ID stays the same when you change a contact flow, you can use the logs to compare the interactions with different versions of the contact flow.

The following example log entry shows a Set working queue block of a customer queue flow.

```
{
    "Timestamp": "2017-11-09T12:17.898Z",
    "ContactId": "f0b21968-952b-47ba-b764-f29a57bcf626",
    "ContactFlowId": "arn:aws:connect:us-east-2:0123456789012:instance/d-92673ef055/contact-flow/b1d791cf-1264-42e3-9a73-62c8b3c9a45",
    "ContactFlowModuleType": "SetQueue",
    "Events": {
        "Queue": [
            "arn:aws:connect:us-east-2:670047220557:instance/d-92673ef044/queue/f0300e43-9547-477c-b8ba-0bb72e7fa1"
        ]
    }
}```
Track customers between contact flows

In many cases, customers interact with multiple contact flows in your contact center, being passed from one contact flow to another to appropriately assist them with their specific issue. Contact flow logs help you track customers between different contact flows, by including the ID of the contact in each log entry.

When a customer is transferred to a different contact 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 contact flow.

In larger, high-volume contact centers, there can be multiple streams for contact flow logs. If a contact is transferred to a different contact 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 contact flow log events

You can configure CloudWatch to define a filter pattern that looks for specific events in your contact 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 contact 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 contact flows.

Contact block definitions

You create contact flows in the contact flow designer using contact blocks. Drag and drop contact blocks onto a canvas to arrange a contact flow.

The following table lists all available contact blocks that you can use. Choose the links in the Block column for more information.

<table>
<thead>
<tr>
<th>Block</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call phone number (p. 203)</td>
<td>Initiates an outbound call from an outbound whisper flow.</td>
</tr>
<tr>
<td>Change routing priority / age (p. 205)</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>Check contact attributes (p. 207)</td>
<td>Checks the values of contact attributes.</td>
</tr>
<tr>
<td>Check hours of operation (p. 210)</td>
<td>Checks whether the contact is occurring within or outside of the hours of operation defined for the queue.</td>
</tr>
<tr>
<td>Check queue status (p. 211)</td>
<td>Checks the status of the queue based on specified conditions.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Check staffing (p. 213)</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>Disconnect / hang up (p. 215)</td>
<td>Terminates a customer contact.</td>
</tr>
<tr>
<td>Distribute by percentage (p. 215)</td>
<td>Routes customers randomly based on a percentage.</td>
</tr>
<tr>
<td>End flow / Resume (p. 217)</td>
<td>Ends the current flow without disconnecting the contact.</td>
</tr>
<tr>
<td>Get customer input (p. 218)</td>
<td>Branches based on customer intent.</td>
</tr>
<tr>
<td>Get queue metrics (p. 225)</td>
<td>Retrieves real-time metrics about queues and agents in your contact center and returns them as attributes.</td>
</tr>
<tr>
<td>Hold customer or agent (p. 230)</td>
<td>Places a customer or agent on or off hold.</td>
</tr>
<tr>
<td>Invoke AWS Lambda function (p. 231)</td>
<td>Calls AWS Lambda, optionally returns key-value pairs.</td>
</tr>
<tr>
<td>Loop (p. 233)</td>
<td>Loops through, or repeats, the Looping branch for the number of loops specified.</td>
</tr>
<tr>
<td>Loop prompts (p. 234)</td>
<td>Loops a sequence of prompts while a customer or agent is on hold or in queue.</td>
</tr>
<tr>
<td>Play prompt (p. 236)</td>
<td>Plays an interruptible audio prompt, delivers a text-to-speech message, or delivers a chat response.</td>
</tr>
<tr>
<td>Set callback number (p. 240)</td>
<td>Sets a callback number.</td>
</tr>
<tr>
<td>Set contact attributes (p. 242)</td>
<td>Stores key-value pairs as contact attributes.</td>
</tr>
<tr>
<td>Set customer queue flow (p. 244)</td>
<td>Specifies the flow to invoke when a customer is transferred to a queue.</td>
</tr>
<tr>
<td>Set disconnect flow (p. 245)</td>
<td>Sets the flow to run when the agent disconnects from the chat.</td>
</tr>
<tr>
<td>Set hold flow (p. 247)</td>
<td>Links from one contact flow type to another.</td>
</tr>
<tr>
<td>Block</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set recording and analytics behavior (p. 249)</td>
<td>Sets options for recording conversations.</td>
</tr>
<tr>
<td>Set voice (p. 251)</td>
<td>Sets the text-to-speech (TTS) language and voice to be used in the contact flow.</td>
</tr>
<tr>
<td>Set whisper flow (p. 253)</td>
<td>Overrides the default whisper by linking to a whisper flow.</td>
</tr>
<tr>
<td>Set working queue (p. 256)</td>
<td>Specifies the queue to be used when Transfer to queue is invoked.</td>
</tr>
<tr>
<td>Start media streaming (p. 258)</td>
<td>Starts capturing customer audio for a contact.</td>
</tr>
<tr>
<td>Stop media streaming (p. 260)</td>
<td>Stops capturing customer audio after it is started with a Start media streaming block.</td>
</tr>
<tr>
<td>Store customer input (p. 261)</td>
<td>Stores numerical input to a contact attribute.</td>
</tr>
<tr>
<td>Transfer to agent (beta) (p. 264)</td>
<td>Transfers the customer to an agent.</td>
</tr>
<tr>
<td>Transfer to flow (p. 265)</td>
<td>Transfers the customer to another contact flow.</td>
</tr>
<tr>
<td>Transfer to phone number (p. 267)</td>
<td>Transfers the customer to a phone number external to your instance.</td>
</tr>
<tr>
<td>Transfer to queue (p. 270)</td>
<td>In most contact flows, this block ends the current contact 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>Wait (p. 274)</td>
<td>Pauses the contact flow.</td>
</tr>
</tbody>
</table>

**Contact block: Call phone number**

**Description**

- Use to place an outbound call from an Outbound Whisper flow.

**Contact flow types**

You can use this block in the following contact flow types (p. 170):
• Outbound Whisper flow

Properties

Call phone number

Initiates a call to a customer. You can optionally set the caller ID number to display to the recipient.

If you do not specify a caller ID number, the caller ID number for the queue is displayed. Learn more

☐ Caller ID number to display (optional)

☐ Select a number from your instance

Number

Search for phone number

☐ ☐ +1 7

☐ ☐ +1 8

☐ ☐ Caller ID number to display (optional)

☐ Select a number from your instance

☐ Use attribute

Type

User Defined

Attribute

MainPhoneNumber
Configured block

When this block is configured, it looks similar to the following image:

Sample flows

See these sample flows for scenarios that use this block:

- Sample customer queue priority (p. 163)
- Sample queue configurations (p. 163)

Scenarios

See these topics for more information about caller ID works:

- How caller ID works in Call phone number block (p. 125)
- Set up outbound caller ID (p. 124)

Contact block: Change routing priority / age

Description

- Change a customer's position in the queue.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Outbound Whisper flow
- Inbound contact flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow
This block gives you two options for changing a customer'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.
Configured block

When this block is configured, it looks similar to the following image:

Sample flows

See these sample flows for scenarios that use this block:

- Sample customer queue priority (p. 163)
- Sample queue configurations (p. 163)

Scenarios

See these topics for more information about how routing priority works:

- Routing profiles (p. 14)
- How routing works (p. 119)

Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- All flows
Properties

Check contact attributes

Branches based on a comparison to the value of a contact attribute.

Examples of supported comparisons include: "equal to", "greater than", "less than" "starts with", "ends with", "contains".

Attribute to check

**Type**
- User Defined

**Attribute**
- PremiumCustomer

**Conditions to check**

<table>
<thead>
<tr>
<th>x</th>
<th>Equals</th>
<th>Yes</th>
</tr>
</thead>
</table>

No Match

Add another condition

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 Amazon Connect compares the **greater than 60** condition first and compares **greater than 2** last.
Configured

When this block is configured, it looks similar to the following image:

Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 162)
- Sample interruptible queue flow with callback (p. 167)

Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes (p. 281)
- How to use the Channel contact attribute (p. 285)
- How to use contact attributes to personalize the customer experience (p. 278)
Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

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 (p. 122).

Configuration tips

- Agent queues (p. 15) 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

When this block is configured, it looks similar to the following image:

Related topics

• Set the hours of operation and timezone for a queue (p. 122)

Sample flows

Sample inbound flow (first contact experience) (p. 162)

Scenarios

See these topics for scenarios that use this block:

• Manage contacts in a queue (p. 187)

Contact 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.
• If no match is found, the No Match branch is followed.

Contact flow types

You can use this block in the following contact flow types (p. 170):
• Inbound contact flow
• Customer queue flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

Check queue status

Branches based on the comparison of Time in Queue or Queue capacity. If no match is found, the No Match branch is followed.

Outputs:

<table>
<thead>
<tr>
<th>Time in Queue</th>
<th>▼</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Is greater than ▼ 1 min. ▼</td>
<td></td>
</tr>
</tbody>
</table>

• No Match
• Error

Add another condition

☐ Queue to check (optional)

☐ By queue

☐ Select a queue

BasicQueue □ ▼

☐ Use attribute

☐ By agent

Configured block

When this block is configured, it looks similar to the following image:
Check staffing

**Scenarios**

See these topics for scenarios that use this block:

- Manage contacts in a queue (p. 187)

**Contact block: Check staffing**

**Description**

- Checks the current working queue, or queue you specify in the block, for whether agents are available (p. 443), staffed (p. 448), or online (p. 447).
- 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.

**Contact flow types**

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

Check staffing

Branches based on whether agents are available, staffed (e.g. available, on call, or after call work), or online.

Status to check

Available

Queue to check (optional)

By queue

Select a queue

BasicQueue

Use attribute

By agent

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 in the Available or Staffed state, or if they are Offline.

Configuration tips

• You must set a queue before using a Check staffing block in your contact flow. You can use a Set working queue (p. 256) 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 contact flow is passed from that flow to the next flow.

Configured block

When this block is configured, it looks similar to the following image:
Scenarios

See these topics for scenarios that use this block:

- Transfer contacts to a specific agent (p. 188)

Contact block: Disconnect / hang up

Description

- Disconnects the customer.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Contact block: Distribute by percentage

Description

- This block is useful for doing A/B testing. It routes customers randomly based on a percentage.
- Like flipping a coin, contacts are distributed randomly, which doesn't guarantee exact percentage splits.

Contact flow types

You can use this block in the following contact flow types (p. 170):
• Inbound contact flow
• Customer queue flow
• Outbound Whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

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 contact a is being routed through a flow, Amazon Connect generates the random number.

- If 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

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:

- Sample AB test (p. 162)

Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Customer queue flow
- Customer whisper flow
- Outbound Whisper flow
- Agent whisper flow
Properties

End flow / Resume

Ends the current flow without disconnecting the caller.

For example, this can be used to return to Loop prompts when it has been interrupted.

When End flow / return from interruption is invoked, the customer will remain connected to the system.

Configured block

When this block is configured, it looks similar to the following image:

Contact 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, 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

• Inbound contact flow
• Customer queue flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

Get customer input

Delivers an audio or chat message for a customer response.

The contact flow branches based on the customer input: DTMF, chat, or Amazon Lex. Learn more.

☐ Select from the prompt library (audio)
  ☐ Select a prompt
    Audio prompt
    Search for prompt

☐ Select dynamically

☐ Text-to-speech or chat text

DTMF ☐ Amazon Lex

Plays an audio prompt and branches based on DTMF or Amazon Lex intents. The audio prompt is interruptible when using DTMF.

Set timeout (Minimum one second)
5 seconds

Add another condition

You can configure this block to accept DTMF input, a chat response, or an Amazon Lex intent.
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.

Amazon Lex tab properties

- **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.

  Important
  In a production environment, always use a different alias than $LATEST. Only use $LATEST for manual testing. If the bot alias is $LATEST Lex invocations are throttled. For more information, see Runtime Service Quotas.

- **Session attributes**: Specify attributes that apply to the current contact’s session only.
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.

- **Max Speech Duration**
  
  \[
  \text{x-amz-lex:max-speech-duration-ms:[intentName]:[slotToElicit]} \]

  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 = 13000 milliseconds (13 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**
  
  \[
  \text{x-amz-lex:start-silence-threshold-ms:[intentName]:[slotToElicit]} \]

  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 = 4000 milliseconds (4 seconds).

- **End Silence Threshold**
  
  \[
  \text{x-amz-lex:end-silence-threshold-ms:[intentName]:[slotToElicit]} \]
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)

**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.

To set up this functionality, set the `barge-in-enabled` session attribute in the Get customer input block that calls your Lex bot. This attribute only controls Amazon Lex barge-in; it doesn't control DTMF barge-in.

- **Barge-in**
  
  `x-amz-lex:barge-in-enabled:[intentName]:[slotToElicit]`

  Barge-in is disabled globally by default. You must set the session attribute to enable it at the global, bot, or slot levels. For more information, see How to use Lex session attributes (p. 286).

**Intents**

- Enter the intents you created in Amazon Lex. They are case sensitive!
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 contact flow.

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. It's not possible to configure Lex to wait a shorter length of time.

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 contact flow.

For example, you have a Get_Account_Number bot. In the contact 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.

**Configured block**

When this block is configured, it looks similar to the following image:

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**

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 162)
- Sample interruptible queue flow with callback (p. 167)
- Sample queue configurations (p. 163)
- Sample recording behavior (p. 168)

**Scenarios**

See these topics for scenarios that use this block:

- Add an Amazon Lex bot (p. 332)
- How to use the same bot for voice and chat (p. 287)
- Add text-to-speech to prompts (p. 174)
Contact block: Get queue metrics

Description

• Retrieves the following real-time metrics 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.
  • Queue name (p. 448)
  • Queue ARN.
  • Contacts in queue (p. 447)
  • Oldest contact in queue (p. 447)
  • Agents online (p. 447)
  • Agents available (p. 443)
  • Agents staffed (p. 448)
  • Agents after contact work (p. 441)
  • Agents busy (p. 447)
  • Agents missed (p. 442) (Agent non-response)
  • Agents non-productive (p. 447)
• 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 (p. 207) 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

• All flows
Properties

Optional parameters:

- Set channel
  - Filter by
    - Voice
    - Chat
  - Use attribute
- Set queue

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, if you choose the following settings, *Get queue metrics* would return metrics for only the BasicQueue, filtered to include only chat contacts.
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 (p. 242) 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.
Set contact attributes

Stores key / value pairs as contact attributes.
Contact attributes are accessible by other areas of Amazon Connect, such as the Contact Control Panel (CCP) and Contact Trace Records (CTRs). Learn more

Attribute to save

- Use text
  - Destination key
    - CustomerSpecified
  - Value
    - chat
- Use attribute

Using the Check contact attributes block after the Get queue metrics block

After a Get queue metrics block, add a Check contact attributes (p. 207) 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 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.
Configured block

When this block is configured, it looks similar to the following image:

Scenarios

See these topics for scenarios that use this block:
• Checking attribute values in a Check contact attributes block (p. 282)

Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):
• Inbound contact flow
• Outbound Whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The following settings are available:

• 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**

When this block is configured, it looks similar to the following image:

![Hold customer or agent](image)

**Samples flows**

Sample secure input with agent (p. 169)

**Contact 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.

**Contact flow types**

You can use this block in the following contact flow types (p. 170):

- Inbound contact 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

Invoke AWS Lambda function

Makes a call to AWS Lambda, and optionally returns key / value pairs.

The returned key value pairs can be used to set contact attributes.

Function ARN

- Select a function
  am:aws:lambda:us-xxxx:x:function:state

- Use attributes

Function input parameters

Add a parameter

Timeout (max 8 seconds)

4

Note the following properties:

- **Timeout**: Enter how long to wait for Lambda to time out. This creates a branch for you to specify what to do if it times 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.

Configuration tips

- To use an AWS Lambda function in a contact flow, first add the function to your instance. For more information, see Add a Lambda function to your Amazon Connect instance (p. 339),
• 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 contact flow.

Configured block

When this block is configured, it looks similar to the following image:

![Sample Lambda integration](image)

Sample flows

Sample Lambda integration (p. 168)

Scenarios

See these topics for scenarios that use this block:

• Invoke AWS Lambda functions (p. 339)

Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

• All flows
Loop prompts

Properties

- **Loop**

Loops through (repeats) the Looping branch for the number of loops specified. After the loops are completed, the Complete branch is followed. If you enter 0 for the loop count, the Complete branch is followed the first time this block executes.

- **Number of loops**
  - 2
  - 0-100

- **Use attribute**

Configuration tips

- If you enter 0 for the loop count, the **Complete** branch is followed the first time this block runs.

Configured block

When this block is configured, it looks similar to the following image:

Contact block: Loop prompts

Description

- Loops a sequence of prompts while a customer or agent is on hold or in queue.
Contact flow types

You can use this block in the following contact flow types (p. 170):

- Customer Queue flow
- Customer Hold flow
- Agent Hold flow

Properties

Loop prompts

Loops a sequence of prompts while a customer or agent is on hold or in queue.

When Loop prompts is used in a queue flow, audio playback can be interrupted with a flow at preset times.

Prompts

- Audio recording
- CustomerHold.wav

Add another prompt to the loop

Interrupt

- Interrupt every 1 Minutes

Configuration tips

- 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 dequeueing 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 contact flow. If you reuse the contact 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 contact 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

When this block is configured, it looks similar to the following image:

![Loop prompts block](image)

Sample flows

See these sample flows for scenarios that use this block:

• Sample interruptible queue flow with callback (p. 167)

Scenarios

See these topics for scenarios that use this block:

• Manage contacts in a queue (p. 187)

Contact block: Play prompt

Description

• This block can play an interruptible 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. However, you can record and upload your audio prompts. For instructions, see Create prompts (p. 173).

Contact flow types

You can use this block in the following contact flow types (p. 170):

• Inbound contact flow
• Customer Queue flow
• Customer Whisper flow
• Agent Whisper flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

The properties give you different ways to choose the prompt to be played:

• **Select from the prompt library (audio):** Choose from one of the pre-recorded prompts included with Amazon Connect, or record and upload (p. 173) your own prompt.

  ![Play prompt](Image)

  Delivers an audio or chat message.

  Enter text for voice or chat responses. You can personalize messages by using attributes.

  Prompt

  • Select from the prompt library (audio)

  • Select a prompt

  Audio prompt

  Search for prompt ▲

  ○ Beep.wav
  ○ CustomerHold.wav
  ○ CustomerQueue.wav
  ○ Music_Jazz_MyTimetoFly_Inst.wav
  ○ Music_Pop_ThisAndThatIsLife_Inst.wav
  ○ Music_Pop_ThrowYourselfInFrontOfIt_Inst.wav
  ○ Music_Rock_EverywhereTheSunShines_Inst.wav

  • Select dynamically:
1. You can select which prompt to play by using an attribute. For example, in the Play prompt block, choose User Defined, and then enter a name for your attribute. In the following example, we use Company_Welcome_Message.

![Select from the prompt library (audio)](image)

2. Add Set contact attributes (p. 242) blocks to your flow. Configure each one to play the appropriate audio prompt. For example, the first one might play the .wav file for 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 (p. 242) block.

![Set contact attributes](image)

3. Connect the Set contact attributes (p. 242) blocks to the Play prompt block.
• **Text-to-speech or chat text:** You have two options:

  • **Enter text:** To play text, Amazon Connect sends it to Amazon Polly, a service that converts text into lifelike speech using Speech Synthesis Markup Language (SSML). Amazon Polly returns the speech to Amazon Connect to play.
• **Enter dynamically:** Upload .wav files that should be played, based on the value of the attribute.

• **Interpret as:** The default setting in a contact flow block for interpreting text-to-speech is Text. To use SSML for text-to-speech in your contact flow blocks, set the **Interpret as** field to **SSML** as shown in the following image.

![Interpret as SSML](image)

When you add a prompt to a contact 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.

To learn which SSML tags Amazon Connect supports, see [SSML tags supported by Amazon Connect](#) (p. 178).

**Configuration tips**

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). You can also specify text in a flow using a contact attribute.

**Configured block**

When this block is configured, it looks similar to the following image:

![Configured block](image)

**Sample flows**

All of the sample flows use the **Play prompt** block. Take a look at the [Sample inbound flow (first contact experience)](#) (p. 162) to see a **Play prompt** for chat and one for audio.

**Contact block: Set callback number**

**Description**

• Specify the attribute to set the callback number.
Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

Set callback number

Specifies the number to be used to call the customer back in the Contact Control Panel (CCP), or when Transfer to queue is invoked with the callback option.

Use attribute

Type

System

Attribute

Stored customer input

Configuration tips

- The Store customer input block often comes before this block. It stores the customer's callback number.

Configured block

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:

- Sample queue configurations (p. 163)
- Sample queued callback (p. 167): this sample only applies to previous instances of Amazon Connect.

Scenarios

See these topics for scenarios that use this block:

- Set up queued callback (p. 191)
- About queued callbacks in metrics (p. 417)

Contact block: Set contact attributes

Description

- Stores key-value pairs as contact attributes.
- Contact attributes are accessible by other areas of Amazon Connect, such as the CTRs.

  For more information about how to use contact attributes, see Use Amazon Connect contact attributes (p. 276).

Contact flow types

You can use this block in the following contact flow types (p. 170):

- All flows
Properties

Set contact attributes

Stores key / value pairs as contact attributes.

Contact attributes are accessible by other areas of Amazon Connect, such as the Contact Control Panel (CCP) and Contact Trace Records (CTR).

Attribute to save

- Use text
  - Destination key: greetingPlayed
  - Value: true

- Use attribute

Add another attribute

Configured block

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:
- Sample inbound flow (first contact experience) (p. 162)

Scenarios

See these topics for scenarios that use this block:
- How to use contact attributes to personalize the customer experience (p. 278)

Contact block: Set customer queue flow

Description

- Specifies the flow to invoke when a customer is transferred to a queue.

Contact flow types

You can use this block in the following contact flow types (p. 170):
- Inbound contact flow
- Transfer to Agent flow
- Transfer to Queue flow

Properties

For information about using attributes, see Use Amazon Connect contact attributes (p. 276).

Configured block

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:

- Sample queued callback (p. 167)

Contact block: Set disconnect flow

Description

- Specifies which contact flow to run after a disconnect event during a conversation. A disconnect event is when an agent disconnects. When the disconnect event occurs, the corresponding content flow runs.

- Here are examples of when you might use this block:
  - Run post-call 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 (p. 218) block. Their answers are uploaded using an Invoke AWS Lambda function (p. 231) block to an external customer feedback database. The customer is thanked and disconnected.

    For more information about creating post-call surveys, see this blog post by an AWS Solution Architect: Create post call surveys in 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 (p. 274) block, or end the conversation.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- All flows
Properties

Set disconnect flow

Specifies the disconnect flow for either agent, customer, or both.

Remaining participants

Customer only

Select a flow

Search for contact flow

Use attribute

Configured block

When this block is configured, it looks similar to the following image:

Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 162)

Scenarios

See these topics for scenarios that use this block:

- Example chat scenario (p. 11)
• Create post call surveys in Amazon Connect

Contact block: Set hold flow

Description

• Links from one contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

• Inbound contact flow
• Customer Queue flow
• Outbound whisper flow
• Transfer to Agent flow
• Transfer to Queue flow
Properties

Set hold flow

Specifies the flow to invoke when a customer or agent is put on hold. Learn more

Hold flow

- Agent
- Select a flow
- Use attribute

Type

- User Defined
- External
- Lex slots
- Lex attributes
- Customer

For information about using attributes, see Use Amazon Connect contact attributes (p. 276).

Configured block

When this block is configured, it looks similar to the following image:
Contact block: Set logging behavior

Description

- Enables contact flow logs.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- All flows

Properties

<table>
<thead>
<tr>
<th>Set logging behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>When logging is enabled, data for each block in your contact flow is sent to Amazon CloudWatch Logs. Learn more</td>
</tr>
<tr>
<td>Logging behavior</td>
</tr>
<tr>
<td>Enable</td>
</tr>
<tr>
<td>Disable</td>
</tr>
</tbody>
</table>

Scenarios

See these topics for more information about contact flow logs:

- Track events as customers interact with contact flows (p. 198)

Contact 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 Amazon Connect. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 378).

Contact flow types

You can use this block in the following contact flow types (p. 170):

• Inbound contact flow
• Customer Queue flow
• Transfer to Agent flow
• Transfer to Queue flow

Properties

Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

Call recording

Enables or disables call recording for the agent, customer, or both. Agent and customer call recordings are required to enable Contact Lens.

- On
- Agent and Customer
- Agent only
- Customer only
- Off

When configuring this block to set up recording behavior (p. 190), 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, see Enable Contact Lens for Amazon Connect (p. 378).

Configuration tips

- Let's say you have a flow that links to a flow that links to another flow. Each flow might have its own Set recording behavior block. The last Set recording behavior block overrides the settings of the previous two Set recording behavior blocks.
For example, you might have a contact flow with **Set recording behavior to record Agent and Customer**. But if the next **Set recording behavior** block is set to **Agent only**, that block overrides the behavior of the previous block.

- 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 CTR. Contact Lens needs to run on that CTR as well.

**Configured block**

When this block is configured, it looks similar to the following image:

![Configured block image](image)

**Sample flows**

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 162)

**Scenarios**

See these topics for scenarios that use this block:

- Set up recording behavior (p. 190)
- Monitor live conversations (p. 367)
- Review recorded conversations (p. 370)
- Analyze conversations using Contact Lens for Amazon Connect (p. 378)

**Contact 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), an Amazon Polly Neural Text-to-Speech (NTTS) voice. Neural voices make automated conversations sound more lifelike by improving the pitch, inflection, intonation, and tempo.

• 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.

### Contact flow types

You can use this block in the following contact flow types (p. 170):

• All flows

### Properties

**Set Voice**

Specify the language and voice that the customer hears during text-to-speech interactions. [Learn more](#)

**Language**

- **English, US**

**Voice**

- **Joanna**

- [Override default speaking style - Standard (Legacy)](#)

  - [Neural speaking style](#)
    - None

  - [Standard (Legacy)](#)
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

When this block is configured, it looks similar to the following image:

![Set voice block](image)

Scenarios

See these topics for scenarios that use this block:

- Add text-to-speech to prompts (p. 174)

Contact 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 (p. 159) or customer whisper flow (p. 159) 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 (p. 159).

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** (p. 258)/**Stop** (p. 260) media streaming or **Set voice** (p. 251), chat skips these blocks and triggers an error branch. However, it doesn’t prevent the contact flow from progressing.
- Whisper flows don’t appear in transcripts.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

Set whisper flow

Specifies the whisper played to a customer or agent for inbound and outbound calls. Learn more

Whisper flow

○ To Agent

○ To Customer

○ Select a flow

Default customer whisper

○ Use attribute

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 (p. 276).

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 contact flow.

• If you use a Play prompt (p. 236) 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.

Configured block

When this block is configured, it looks similar to the following image:
Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

Set working queue

Specifies the queue to be used when Transfer to queue is invoked.

A queue must be specified prior to invoking Transfer to queue. It's also the default queue for checking attributes, such as: staffing, queue status, and hours of operation.

Outputs:

- By queue
  - Select a queue
    - BasicQueue
  - Use attribute
  - By agent

Note the following properties:

- **By queue > Use attribute.** 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, .../queue/aaaaaaaa-bbbb-cccc-dddd-111111111111.

**Configured block**

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:

- Sample queue customer (p. 166)
- Sample queue configurations (p. 163)

Scenarios

See these topics for scenarios that use this block:

- Set up agent-to-agent transfers (p. 183)
- Transfer contacts to a specific agent (p. 188)

Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
- Customer Whisper flow
- Outbound Whisper flow
- Agent Whisper flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

Start media streaming

Starts streaming media to Kinesis. Learn more
Only audio is supported

**Select stream to start**

- From the customer
- To the customer

**Configuration tips**

- You must enable live media streaming in your instance to successfully capture customer audio. For instructions, see Capture customer audio: live media streaming (p. 346).
- Customer audio is captured until a Stop media streaming block is invoked, even if the contact is passed to another contact 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**

When this block is configured, it looks similar to the following image:

![Configured block](image)

**Sample flows**

Example contact flow for testing live media streaming (p. 353)
Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact 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 Capture customer audio: live media streaming (p. 346).
- Customer audio is captured until a Stop media streaming block is invoked, even if the contact is passed to another contact flow.
- If this block is triggered during a chat conversation, the contact is routed down the Error branch.

Configured block

When this block is configured, it looks similar to the following image:
Sample flows

Example contact flow for testing live media streaming (p. 353)

Contact block: Store customer input

Description

This block is similar to Get customer input, but this one stores the input as a contact attribute and allows you to encrypt it. This way, you can encrypt sensitive input such as credit card numbers. This block:

- Plays an interruptible 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 a contact attribute.
- Allows you to specify a custom terminating keypress.
- If this block is triggered during a chat conversation, the contact is routed down the Error branch.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow
Properties

Store customer input

Stores numerical input to contact attribute.

Plays an interruptible audio prompt and stores digits via DTMF as a contact attribute. Learn more

Prompt

- Select from the prompt library (audio)
  - Select a prompt
    - Audio prompt
      - Search for prompt
  - Select dynamically
- Text-to-speech or chat text

Customer input

- Custom
  - Maximum Digits: 20
  - Timeout before first entry: 5 seconds in seconds
  - Encrypt entry (recommended)
  - Specify terminating keypress Learn more.
  - Disable cancel key Learn more.
- Phone number

Note the following properties:
• **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. 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 #.

• **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* (p. 231) 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.

**Configuration tips**

To use a star (*) as part of the terminating keypress, you must also choose **Disable cancel key**.

**Configured block**

When this block is configured, it looks similar to the following image:
Sample flows

See these sample flows for scenarios that use this block:

- Sample secure input with agent (p. 169)
- Sample secure input with no agent (p. 169)
- Sample queue configurations (p. 163)
- Sample queued callback (p. 167)

Scenarios

Creating a secure IVR solution with Amazon Connect

Contact block: Transfer to agent (beta)

Description

- Ends the current contact flow and transfers the customer to an agent. If the agent is already with someone else, the contact is disconnected.
- The Transfer to Agent block is a beta feature and works only for voice interactions.
- We recommend using the Set working queue (p. 256) 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 (p. 183).

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Transfer to Agent flow
- Transfer to Queue flow
Properties

Transfer to agent (beta)

Ends the current contact flow and transfers the customer to an agent.

This should be used with warm transfers. If the target agent is on a call or unavailable, the transfer will fail and the customer will remain with the original agent.

Transfer

Configured block

When this block is configured, it looks similar to the following image:

Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers (p. 178)

Contact block: Transfer to flow

Description

- Ends the current contact flow and transfers the customer to a different contact flow.

Contact flow types

You can use this block in the following contact flow types (p. 170):
Transfer to flow

- Inbound contact flow
- Transfer to Agent flow
- Transfer to Queue flow

**Properties**

```
Transfer to flow

Ends the current flow and transfers the customer to a flow of type contact flow.

Transfer

○ Select a flow
  Sample customer queue...  x

○ Use attribute
```

**Configured block**

When this block is configured, it looks similar to the following image:

```
Transfer to flow

To Sample customer queue...

Error
```

**Sample flows**

See these sample flows for scenarios that use this block:

- Sample AB test (p. 162)

**Scenarios**

See these topics for scenarios that use this block:

- Set up contact transfers (p. 178)
Contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
- Transfer to Agent flow
- Transfer to Queue flow
## Properties

**Transfer to phone number**

Transfers the customer to a phone number.

**Transfer to**

- Phone number

<table>
<thead>
<tr>
<th>Country code</th>
<th>Phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>🇺🇸 +1</td>
<td></td>
</tr>
</tbody>
</table>

- Use attribute

**Set timeout**

- Timeout (in seconds)

| 30 |

- Use attribute

**Resume contact flow after disconnect**

Adds success, call failed and timeout output branches.

- Yes
  - No

**Optional parameters:**

- Send DTMF
- Caller ID number
- Caller ID name
Note the following properties:

- **Resume contact 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 contact 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 poor audio quality, delay, latency, and displaying the incorrect caller ID.

- **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 Why your caller ID might not appear correctly to customers (p. 126).

**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 allow list for making the call, it will fail. For more information, see Countries you can call (p. 569).

- 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 contact flow when the call is transferred, or choose to **Resume contact flow after disconnect**, which returns the caller to your instance and resumes the contact flow after the transferred call ends.

**Configured block**

When this block is configured, it looks similar to the following image:
Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers (p. 178)
- Set up outbound caller ID (p. 124)

Contact block: Transfer to queue

Description

- In most types of contact flows, this block ends the current contact 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.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact 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
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 (p. 121) 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**
Transfer to queue

Ends the current contact flow and transfers the customer to a queue. Learn more

Transfer to queue  Transfer to callback queue

When you use Transfer to callback queue, you must use a 'Set customer callback number' block before this block in the flow to set the callback number for the customer.

Initial delay

99

in seconds

Max number of retries  Minimum time between attempts

2  10

minutes  0

seconds

Optional parameters:

- Set working queue
  - By queue
    - Select a queue
      - Search for queue
  - Use attribute
  - By agent

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 contact 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 contact 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 contact 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. 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. 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 (p. 187)
- Set up queued callback (p. 191)
- About queued callbacks in metrics (p. 417)

Sample flows

See these sample flows for scenarios that use this block:

- Sample queue configurations (p. 163)
- Sample customer queue priority (p. 163)
- Sample queued callback (p. 167)

Contact block: Wait

Description

- Use this block in chat contact flows only. If a contact stops responding to a chat, this block pauses the contact flow for the specified wait time.
- If this block is triggered during a voice conversation, the contact is routed down the Error branch.

Contact flow types

You can use this block in the following contact flow types (p. 170):

- Inbound contact flow
- Customer Queue flow
Properties

It has two properties:

- **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. Maximum is 24 hours.
- **Customer return**: Run 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.

**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 contact flow that puts them in a priority queue. However, it doesn't route them to the same agent.

**Configured block**

When this block is configured, it looks similar to the following image:
Use Amazon Connect contact attributes

In Amazon Connect, a contact is an interaction with a customer in your contact center. The interaction can be a voice phone call, a chat, or an automated interaction using an Amazon Lex bot. Contact attributes in Amazon Connect refer to key-value pairs that contain data about a contact.

Using contact attributes, you can customize and personalize the experience customers have when they interact with your contact center. Contact attributes let you store customer input or data about a customer, and then use it later in a contact flow. You can also check the values of contact attributes and use a condition to determine the branching behavior of the contact flow based on the value.

Contact attributes let you pass data between Amazon Connect and other services, such as Amazon Lex and AWS Lambda. Contact attributes can be both set and consumed by each service. For example, you could use a Lambda function to look up customer information, such as their name or order number, and use contact attributes to store the values returned to Amazon Connect. You could then reference those attributes to include the customer's name in messages using text to speech, or store their order number so they do not have to enter it again.

Contents

- Contact attribute concepts (p. 277)
- Types of contact attributes (p. 277)
- How to use contact attributes to personalize the customer experience (p. 278)
- Use Amazon Connect contact attributes with other services (p. 280)
- Use contact attributes in the CCP (p. 281)
Contact attribute concepts

When you create a contact flow, you can create user-defined contact attributes using **Set contact attributes** blocks. You can then reference them in other parts of a contact flow using any other block that supports dynamic attributes. For example, you could use a **Check contact attributes** block to compare the value of an attribute to a condition you define, and then route the contact based on the results of the comparison. You could also retrieve data from external sources, and then create user-defined attributes from the external data so that you can reference them later in a contact flow, such as the status of an order or an expected shipping date.

Personalize the customer experience by including the customer's name when you use text to speech text in a **Play prompt** or **Get customer input** block to speak messages to your customer. Use contact attributes to store input provided by a customer during an interaction with an Amazon Lex bot to enable automated interactions.

As a best practice, make attributes and attribute values case-sensitive, and always match case in each context where they are used.

Types of contact attributes

The following types of contact attributes are available in Amazon Connect.

System contact attributes

These are predefined attributes in Amazon Connect. You can reference system attributes, but you cannot create them.

Some system attributes relate to contacts, and some relate to metrics. Not all blocks in a contact 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.

Agent contact attributes

A subset of system attributes related to agents in your contact center.

Agent attributes are available only in the following types of contact flows:

- Agent whisper
- Customer whisper
- Agent hold
- Customer whisper
- 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 contact flow types:
• Customer queue
• Transfer to queue
• Inbound contact flow

Queue metrics contact attributes

These are System metric attributes returned when you use a `Get queue metrics` block in your contact flow.

User-defined contact attributes

These attributes are created when a contact flow runs using `Set contact attributes` blocks. When you get data from an external source, you can copy key-value pairs as user-defined attributes to reference later in a contact flow. You can also create user-defined attributes through the Amazon Connect API.

User-defined attributes include all attributes set by using a `Set contact attributes` block in a contact flow. User-defined attributes are included in contact trace records (CTRs). They are available to Lambda functions that are invoked after the `Set contact attributes` block, and are created in the Attributes namespace. They are also available to applications that integrate with the Contact Control Panel (CCP) for screenpop information, and can be referenced in contact flows.

External contact attributes

External—Attributes are created via a process external to Amazon Connect. For example, when you use an `Invoke AWS Lambda function` block in a contact flow, or integrate with an Amazon Lex bot.

External 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. You can access external attributes in contact flows via `$.External.AttributeName`. For more information about using attributes in Lambda functions, see Using AWS Lambda Functions with Amazon Connect.

These attributes are not included in CTRs, 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 via the `Set contact attributes` block. When used in `Set contact attributes` blocks, the attributes that are copied are included in CTRs, and can be used in the CCP.

Lex slots contact attributes

External attributes for the slot name of an Amazon Lex bot.

Lex attributes

Session attributes from an Amazon Lex bot interaction.

How to use contact attributes to personalize the customer experience

Contact attributes in your contact flows can provide a more personalized customer experience. For example, specify a custom flow based on comparing an attribute to a value. You then route the contact based on the value comparison, such as routing customers to different tiers of support based on their account number. Or retrieve a customer’s name and save it as an attribute. Include the name attribute in a text to speech string so that the customer’s name is said during the interaction.
Tip
Contact attributes are shared across all contacts with the same InitialContactId. This means that while carrying out transfers, for example, a contact attribute updated in the transfer flow updates the attribute's value in both CTR's contact attributes (that is, the Inbound and Transfer contact attributes).

The steps in the following sections describe how to use contact attributes with different blocks in a contact flow.

Using a Set contact attributes block

Use a **Set contact attributes** block to set a value that is later referenced in a contact 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 contact 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.

Using attributes with a Lambda function

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 contact 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 contact 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 contact 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 contact 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 the **Type**, choose **External**.

9. For **Attribute** type 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 contact 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 contact 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 contact 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 contact 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.

"$" 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.

Use Amazon Connect contact attributes with other services

You can reference contact attributes set in your Amazon Connect contact flow in other services, such as in an Amazon Lex bot or AWS Lambda function. This allows data associated with the customer or the contact to be shared between services.
To use contact attributes to access other resources, set a user-defined attribute in your contact flow and use the Amazon Resource Name (ARN) of the resource you want to access as the value for the attribute.

For example, 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.

**Use contact attributes in the CCP**

Contact attributes also let you capture information and then present that information in a screenpop to an agent in the Contact Control Panel (CCP). Use contact attributes 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 via 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 contact flow named “Sample note for screenpop.” In this contact 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.

**How to reference contact attributes**

The way you reference contact attributes depends on how they were created and how you are accessing them. 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.

For example, to reference a customer name from a Lambda function lookup, you use $.External.AttributeKey, replacing AttributeKey with the key (or name) of the attribute returned from the Lambda function. 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.

To reference user-defined attributes, such as those set with the **Set contact attributes** block, use the drop-down menus in subsequent blocks to reference the attribute, or use the Attributes namespace in JSONPath to the attribute if used in a text field. For example, if you create a user-defined attribute in a **Set contact attributes** block, you reference it in one of the following ways:

- In a block that supports attributes, such as a **Check contact attributes** block, choose User Defined for the Type, and use the value you entered for the Destination key in the Attribute field.
- In a text field in a block, such as a **Play prompt** block, use the JSONPath $.Attributes.DestinationKey, replacing DestinationKey with the value you entered in the Destination key.

JSONPath is a standardized way to query elements of a JSON object. JSONPath uses path expressions to navigate elements, nested elements, and arrays in a JSON document. For more information about JSON, see Introducing JSON.
Checking attribute values in a Check contact attributes block

When you include a Check contact attributes block in a contact flow, it checks the value of the attribute you specify. You then add a condition to compare the value of the attribute to, such as "greater than" or "contains." For each condition you add, an output branch is added to the block. You can then route the contact based on the conditions by connecting the output branch for the condition to the next block in the contact flow. For example, you can check the current number of customers in a queue, then route the contact to the queue if the active contacts are fewer than 5. You can also route the contact to another different queue if the number of active contacts is more than 5. You can use whichever metrics or attributes you want to make routing decisions as appropriate for your needs. The following procedure describes how to check for the number of contacts in a queue and then route the contact to a queue that has fewer than 5 active contacts in it.

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 contact 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 Branch, 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 contact 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.

Referencing attributes from a 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.

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.

### Getting customer input using an Amazon Lex bot

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 contact flow.

**Using an Amazon Lex bot to get customer input**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. Open an existing or create a new contact flow.
3. Under **Interact**, drag a **Get customer input** block to the designer.
4. Choose the title of the block to display the block settings, then select **Text to speech (Ad hoc)**.
5. 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.
6. Choose the **Amazon Lex** tab, then from the drop-down menu, choose the Amazon Lex bot to use to get customer input.
7. By default, the **Alias** field is populated with $LATEST. To use a different alias of the bot, enter the alias value to use.
8. 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.

9. 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.

10. Choose Save.

How to use system metric attributes

Amazon Connect includes system metric attributes that can help you define routing conditions in your contact flows based on real-time metrics about the queues and agents in your contact center. When you include a Get queue metrics block in your contact flow, metrics are retrieved for the current working queue, or other queue that you specify, and returned as attributes that you can reference in blocks that occur after that block in the flow.

You can reference the metric attributes returned to determine the optimal route for a contact. Check the current queue metrics, such as the number of contacts or available agents in a queue, and how long the oldest contact has been in a queue. You could even get metrics for multiple queues and use a Set contact attributes block to store the metric attributes for each queue. You could then 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. To learn more about the metric attributes available, see System metrics attributes (p. 291).

To use system metrics attributes in a contact flow

1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing contact flow, or create a new one.
3. Add a Get queue metrics block to the contact flow.
4. Optionally, to specify a queue select the Set queue check box and do one of the following:
   • Select the queue to retrieve metrics for from the drop-down list.
   • Select Use attribute, then select the attribute to use.

   If you do not select a queue, metrics are retrieved for the current working queue.
5. Add a Check contact attributes block and connect the Success branch of the Get queue metrics block to it.
6. Choose the title of the Check contact attributes block to display the properties for the block.
7. Under Attribute to check, in the Type drop-down menu, choose Queue metrics. In the Attribute drop-down menu, select the attribute to check.
8. To create a branching condition based on the value of the metric attribute, choose Add another condition.
9. For the Conditions to check, choose the conditions to compare the attribute value to, and then enter a value in the Value field.
10. Add additional blocks to the contact flow, connecting the branch of the Check contact attributes block to route the contact to the next block in the flow.
11. Save and publish the contact flow to make it available in your contact center.

System attributes for contact flows

When creating a contact flow, use the following system attributes in Amazon Connect:

• Customer number—The phone number of the customer. When used in an outbound whisper flow, this is the number that the agents dialed to reach the customer. When used in inbound flows, this is the
number from which the customer placed the call. This attribute is included in the CTRs and Lambda input object under CustomerEndpoint.

- **Dialed number**—The number that the customer dialed to reach your contact center. This attribute is included in the CTRs and Lambda input under SystemEndpoint.

- **Customer callback number**—The number that the system uses to call the customer back, either for the 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. The value can be overwritten with the Set callback number block. This attribute is not included in CTRs, and 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 CTRs. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block, which is not included in CTRs.

- **Stored customer input**—The attribute values created from the most recent Store customer input block invocation. This attribute is not included in CTRs, 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 CTRs. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block, which is not included in CTRs. This attribute value applies only to the most recent invocation of the Lambda function. The value is overwritten with the next invocation of the function.

- **Queue name**—The name of the queue.

- **Queue ARN**—The ARN of the queue.

- **Queue outbound number**—The Outbound caller ID number selected for the queue.

- **Text to speech voice**—The Amazon Polly voice used for text to speech in a contact flow.

- **Contact id**—The unique identifier for the contact.

- **Initial contact id**—The unique identifier for the contact associated with the first interaction between the customer and your contact center.

- **Previous contact id**—The unique identifier for the leg of the contact that occurred before the current contact.

- **Channel**—The method used to contact your contact center, either VOICE or CHAT.

- **Instance ARN**—The ARN for your Amazon Connect instance.

- **Initiation method**—Indicates how the contact was initiated. Valid values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, API, and QUEUE_TRANSFER.

## How to use the Channel contact attribute

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 contact flow.
2. Configure the block as shown in the following image:
3. If the customer is contacting you through chat, specify what should happen next.

4. If the customer is contacting you through a call (No Match), specify the next step in the flow.

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.

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 Use attribute. Enter phoneNumber, and set to System, Customer Number, as shown in the following image.
3. Choose **Add another attribute**.
4. Select **Use attribute**. Enter **callType**, **System**, **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.
Contact attributes available in Amazon Connect

The following sections describe the contact attributes available in Amazon Connect.

Contact flow system attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer number</td>
<td>The customer's phone number.</td>
<td>System</td>
<td>$.CustomerEndpoint.Address</td>
</tr>
<tr>
<td>Dialed number</td>
<td>The number the customer dialed to call your contact center.</td>
<td>System</td>
<td>$.SystemEndpoint.Address</td>
</tr>
<tr>
<td>Customer callback number</td>
<td>The number to dial to call back the customer.</td>
<td>System</td>
<td>not applicable</td>
</tr>
<tr>
<td>Stored customer input</td>
<td>An attribute created from the most recent invocation of a Store customer input 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>Text to speech voice</td>
<td>The name of the voice to use for text-to-speech.</td>
<td>System</td>
<td>$.TextToSpeechVoiceld</td>
</tr>
<tr>
<td>Contact id</td>
<td>The unique identifier of the contact.</td>
<td>System</td>
<td>$.ContactId</td>
</tr>
<tr>
<td>Initial contact id</td>
<td>The unique identifier for the first contact a customer had with your contact center. Use the initial contact ID to track contacts between contact flows.</td>
<td>System</td>
<td>$.InitialContactId</td>
</tr>
<tr>
<td>Previous contact id</td>
<td>The unique identifier for the contact before it was transferred. Use the previous contact ID to trace contacts between contact flows.</td>
<td>System</td>
<td>$.PreviousContactId</td>
</tr>
<tr>
<td>Channel</td>
<td>The method of contact, either VOICE or CHAT.</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</td>
<td>System</td>
<td>$.InitiationMethod</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>$.Agent.LastName</td>
</tr>
<tr>
<td>Agent ARN</td>
<td>The ARN of the agent.</td>
<td>System</td>
<td>$.Agent.ARN</td>
</tr>
</tbody>
</table>

### Contact attributes from Amazon Lex

The following table lists the attributes available 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>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>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>

Values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, and API.
### Contact 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>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 contact flow.</td>
<td>External</td>
<td>$.Lex.DialogState</td>
</tr>
<tr>
<td>Intent name</td>
<td>The user intent returned by Amazon Lex.</td>
<td>External</td>
<td>$.Lex.IntentName</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>External</td>
<td>$.Lex.Slots.slotName</td>
</tr>
<tr>
<td>Session attributes</td>
<td>Map of key-value pairs representing the session-specific context information.</td>
<td>External</td>
<td>$.Lex.SessionAttributes.attributeKey</td>
</tr>
</tbody>
</table>

### Contact attributes returned from a Lambda function

Attributes returned as key-value pairs from a Lambda function are external attributes. 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 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.

### System metrics attributes

The metrics attributes in the following table are returned when you use the Get queue metrics block to retrieve metrics for a queue. 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>$.Metrics.Queue.Size</td>
</tr>
<tr>
<td>Oldest contact in queue</td>
<td>For the contact that has been in the queue the</td>
<td>System</td>
<td>$.Metrics.Queue.OldestContactAge</td>
</tr>
</tbody>
</table>
## Contact 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>longest</td>
<td>The length of time that the contact has been in the queue, in seconds.</td>
<td></td>
<td>$.Metrics.Agents.Online.Count</td>
</tr>
<tr>
<td>Agents online</td>
<td>The number of agents currently online, which means logged in and in any state other than offline.</td>
<td>System</td>
<td>$.Metrics.Agents.Available.Count</td>
</tr>
<tr>
<td>Agents available</td>
<td>The number of agents whose state is set to Available.</td>
<td>System</td>
<td>$.Metrics.Agents.Staffed.Count</td>
</tr>
<tr>
<td>Agents staffed</td>
<td>The number of agents currently staffed, which is agents logged in and in Available, ACW, or Busy states.</td>
<td>System</td>
<td>$.Metrics.Agents.AfterContactWork.Count</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>$.Metrics.Agents.Busy.Count</td>
</tr>
<tr>
<td>Agents busy</td>
<td>The number of agents currently active on a contact.</td>
<td>System</td>
<td>$.Metrics.Agents.Missed.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.NonProductive.Count</td>
</tr>
</tbody>
</table>

### 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>$.MediaStreams.Customer.Audio.StreamARN</td>
</tr>
<tr>
<td>Customer audio start timestamp in the</td>
<td>When the customer audio stream started.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StartTimestamp</td>
</tr>
</tbody>
</table>

292
Contact 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>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>$.MediaStreams.Customer.Audio.StopTimestamp</td>
</tr>
<tr>
<td>Customer audio start fragment number</td>
<td>The number that identifies the Kinesis Video Streams fragment, in the stream used for Live media streaming, in which the customer audio stream started.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StartFragmentNumber</td>
</tr>
</tbody>
</table>

**Telephony call metadata attributes**

Telephony metadata provides additional information from telephony carriers that identify the source of the end user before connecting to an agent.

<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 associated with the call.</td>
<td>System</td>
<td>$.Media.Sip.Headers.P-Charge-Info</td>
</tr>
<tr>
<td>From</td>
<td>The identity of the end user associated with the request.</td>
<td>System</td>
<td>$.Media.Sip.Headers.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.Headers.To</td>
</tr>
</tbody>
</table>

**Note**
Telephony metadata is not consistent across all telephony providers. In some cases, this may result in empty values.

**User-defined attributes**

To reference user-defined attributes, such as those set with the Set contact attributes block, use the drop-down menus in subsequent blocks to reference the attribute, or use the Attributes namespace in JSONPath to the attribute if used in a text field. For example, if you create a user-defined attribute in a Set contact attributes block, you reference it in one of the following ways:

- In a block that supports attributes, such as a Check contact attributes block, choose User Defined for the Type, and use the value you entered for the Destination key in the Attribute field.
In a text field in a block, such as a Play prompt block, use the JSONPath $.Attributes.DestinationKey, replacing DestinationKey with the value you entered in the Destination key.

Migrate contact flows to a different instance

Amazon Connect lets you efficiently migrate contact flows to another instance. For example, you might want to expand into new Regions, or move contact flows from your development environment to your production environment.

To migrate a few contact flows, use the import/export feature (p. 197) in the contact flow designer.

To migrate hundreds of contact flows, you need developer skills. You use the following procedure:

1. **Source instance**
   - `ListContactFlow`: Retrieve the Amazon Resource Number (ARN) for the contact flows that you want to migrate.
   - `DescribeContactFlow`: Get information about each contact flow that you want to migrate.

2. **Destination instance**
   - `CreateContactFlow`: Create the contact flows.
   - `UpdateContactFlowContent`: Update the contact flow content.

You can update the information in the contact flows that you migrate. For more information, see *Amazon Connect Flow Language* (p. 294).

Amazon Connect Flow language

This section describes the Amazon Connect Flow language and how to use it. The Flow language is a JSON-based representation of a series of flow actions, and the criteria for moving between them.

We've provided you with the Flow language so you can:

- Efficiently update contact flows that you're migrating from one instance to another.
- Write contact flows rather than drag blocks onto the contact flow designer.

Contents

- Amazon Connect Flow language concepts (p. 294)
- Example contact flow in Amazon Connect Flow language (p. 295)
- Actions in the Amazon Connect Flow Language (p. 296)

Amazon Connect Flow language concepts

The following terms are used in the Flow language.

Contact

Flows can be run in context of a contact. In this case, they are referred to as contact flows.
Participant

Contact flows can additionally be run in a participant context. This allows participant actions—such as playing prompts or getting customer input—to be run. Certain types of contact flows, such as "No participants remaining" disconnect flows and Workitem contact flows, don't have a participant associated.

Action types

Flow actions have the following implicit types associated with them. A type determines when an action is attempted.

- **Contact actions in the Amazon Connect Flow language (p. 299).** These actions are attempted only when the flow is run in context of a contact. They generally result in contact data being manipulated in some way.
- **Flow control actions in the Amazon Connect Flow language (p. 307).** These actions are used only to determine the path through a flow. They have no side effects. Certain data may not be available. For example, contact data isn't available if the action is determining its path based on contact data. These actions generally work in every circumstance.
- **Interactions in the Amazon Connect Flow language (p. 313).** These actions have side effects, but don't require a contact or a participant. Interactions include actions such as invoking an AWS Lambda function. They generally work in every circumstance.
- **Participant actions in the Amazon Connect Flow language (p. 315).** These actions are attempted only when the flow is run in context of a participant. They generally result in an action that the participant experiences, such as playing a prompt or disconnecting.

Example contact flow in Amazon Connect Flow language

The following example shows a simple contact flow that plays a prompt using static text and disconnects.

To learn how to get block identifiers, we recommend creating a new contact flow in Amazon Connect console, and then calling the DescribeContactFlow API for it.

```json
{
   "Version": "2019-10-30", //A string representing the version of the Flow. Currently the only supported version is 2019-10-30.
   "StartAction": "12345678-1234-1234-1234-123456789012", //A string representing the first Action to run when the flow starts running. //In this case, it's the identifier of the Play prompt block. //The value of this field must match the Identifier of an Action in the Actions list.
   "Metadata": { //An object that may be filled in with data as desired.
      "EntryPointPosition": { "X": 88, "Y": 100 },
      "ActionMetadata": { "12345678-1234-1234-1234-123456789012": { //The identifier of the Play prompt block.
         "Position": { "X": 270, "Y": 98
```
Actions in the Amazon Connect Flow Language

An Action is a single step of a flow's run. This topic describes the fields that must be defined.

**Identifier**

A string that must be unique among all Actions within the same Flow. This Identifier can be up to 50 characters long, and can include any characters (including unicode and spaces). They can be opaque or user-friendly.

**Type**

A string that identifies the type of action being performed for a particular step of the Flow. This type must be one of a list of allowable Types, which are covered later.

**Parameters**

An object that defines the customizable behavior of a particular Action block. Each Action has its own format of this Parameters object, which is detailed in the individual Actions definition.
The Parameters object defines customizable behavior for the Action. For example, it defines which Attributes to set or which AWS Lambda function to run. The format differs for each Action type. To find the specific format of a specific Action's Parameter object, see the individual Action's definition below.

Transitions

An object that defines the behavior for choosing the next Action after the current Action completes. Certain Actions terminate, meaning that they finish running the flow when they're run. This is because Transitions must be defined as an empty object.

The Transitions object defines how to proceed to the next Action during flow runtime. This object must have the following fields specified:

NextAction

NextAction is a string that contains the Identifier of the Action that should be run after this Action, if no error or condition is preferentially chosen.

Errors

Errors is a list of error objects. Each error object contains a type or category of error (ErrorType), and the Identifier of the Action that should be run subsequently when that error occurs (NextAction).

Each individual Action supports specific Errors, detailed in the Action's definition later, and the following commonly supported errors:

- NoMatchingError. This is invoked when an error occurs and no other Error matches.
- NoMatchingCondition. This is invoked if no defined condition resolves to true.

Conditions

Conditions are an ordered list that defines a series of checks to evaluate against the Action's result. This result changes per Action and can also change based on Parameters - examples of these are "the number of contacts in queue" for the CheckMetricData Action if the MetricType parameter refers to the NumberOfContactsInQueue, and "the value of the attribute" for the Compare Action. Conditions are evaluated in order, and the first Condition that evaluates to true will result in it being chosen as the Transition to occur, making that Condition's Target the next Action run. The Conditions object is explained in more detail below.

A Condition is a definition of how to evaluate an Action's result, and may evaluate to true or false. The Conditions object on the flow contains an ordered list of objects. Each object contains a NextAction (the Identifier of the Action to be invoked if the Condition evaluates to be true) and the Condition to evaluate:

- NextAction: A string that contains the Identifier of the Action that should be run after this Action if this Condition is the first condition to evaluate to true.
- Condition: An object that defines the evaluation logic.

The Condition object

The Condition object must contain the following fields:

- Operator: A string that indicates which comparison operator that is applied to the Operands. The list of allowed Operators and a description of their logic is defined in the following table.
- Operands: A list of operands to which the Operator is applied. Depending on the Operator, these Operands may be strings or they may be Condition objects. The specific Operator defines which type of Operand is expected, along with the number of Operands expected (some Operators will require
only one Operand, some will support a list of up to ten Operands). Conditions may be nested no more than five Conditions deep, and a single Condition may not contain more than 50 sub-Conditions, regardless of how deeply nested they are.

### List of Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Operand type</th>
<th>Operand count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equals</td>
<td>Returns true if the string specified exactly equals the result.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>TextStartsWith</td>
<td>Returns true if the result, interpreted as text, begins with the specified string.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>TextEndsWith</td>
<td>Returns true if the result, interpreted as text, ends with the specified string.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>TextContains</td>
<td>Returns true if the result, interpreted as text, contains the specified string at least once.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>NumberGreaterThan</td>
<td>Returns true if the result, interpreted as a numeric value, is larger than the specified string. If either the result or the specified string are not numeric, returns false.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>NumberGreaterOrEqualTo</td>
<td>Returns true if the result, interpreted as a numeric value, is larger than or equal to the specified string. If either the result or the specified string are not numeric, returns false.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>NumberLessThan</td>
<td>Returns true if the result, interpreted as a numeric value, is smaller than the specified string. If either the result or the specified string are not numeric, returns false.</td>
<td>String</td>
<td>One</td>
</tr>
<tr>
<td>NumberLessOrEqualTo</td>
<td>Returns true if the result, interpreted as a numeric value, is smaller than the specified string. If either the result or the specified string are not numeric, returns false.</td>
<td>String</td>
<td>One</td>
</tr>
</tbody>
</table>
### Actions

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Operand type</th>
<th>Operand count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a numeric value, is smaller than or equal to the specified string. If either the result or the specified string are not numeric, returns false.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Example Condition

Following is an example of a condition that returns true if the result starts with "ABC":

```json
{
    "Operator": "TextStartsWith",
    "Operands": [
        "ABC"
    ]
}
```

#### Parameter restrictions for actions in the Amazon Connect Flow language

There are several restrictions on parameters. Here's what they mean:

- Must be defined statically. This means that JSONPath cannot be used at all in this value.
- Must be defined statically or as a single valid JSONPath identifier.

  If JSONPath is used, it must be the entirety of the value; you can't specify an input of "My name is $.Name". Further, the JSONPath must be valid - $.Attributes.stuff is okay, $.BadValue is not okay because there's no "BadValue" path on the object used by flows.

- May be defined statically or dynamically. Anything goes. A value of "My name is $.Name" is fine here, as well as a fully static value.

#### Contact actions in the Amazon Connect Flow language

Contact actions are attempted only for flows that run in context of a contact. They generally result in contact data being manipulated in some way.

**Contents**

- CompleteOutboundCall (p. 300)
- DequeueContactAndTransferToQueue (p. 300)
- TransferContactToAgent (p. 301)
- TransferContactToQueue (p. 301)
- UpdateContactAttributes (p. 302)
- UpdateContactCallbackNumber (p. 302)
- UpdateContactEventHooks (p. 303)
- UpdateContactMediaStreamingBehavior (p. 303)
- UpdateContactRecordingBehavior (p. 304)
- UpdateContactRoutingBehavior (p. 305)
Actions

- UpdateContactTargetQueue (p. 305)
- UpdateContactTextToSpeechVoice (p. 306)
- UpdatePreviousContactParticipantState (p. 307)

CompleteOutboundCall

When a flow is run before an outbound call is made as part of an outbound contact, this action calls the outbound destination. If this action is not used, the first participant action implicitly completes the outbound call.

Parameter object

```json
{
    "CallerId": { Optional, an override of the caller ID to present when calling
        "Number": The caller ID number to present when calling. Can either be fully static
            or a single valid JSONPath identifier
        "Name": The caller ID name to present when calling. **This is not currently
            supported on the UI, so it should be treated as unknown but is an area of expansion since
            we should support name anywhere we support number ideally**
    }
}
```

Results and conditions

None.

Errors

None.

Restrictions

This action can be used only when the contact is in the process of making an outbound call, but has not yet called the outbound number.

Corresponding block in the UI

Call phone number (p. 203)

DequeueContactAndTransferToQueue

This action is a combination of a "Dequeue" action and a "TransferContactToQueue" action. This means that a contact in a queue is removed from the queue, a new contact segment is created with the existing contact as its previous contact, and the new contact is placed into the specified queue (referred to as "Queue-to-queue transfer"). If this contact has not been queued, is actively being joined to an agent, or has been routed to an agent, this action fails.

Parameter object

```json
{
    "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be
        specified. Must be either fully statically defined or a single, valid JSONPath identifier.
    "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
        is specified, this may not be specified. Must be either fully statically defined or a
        single, valid JSONPath identifier.
}
```
Results and conditions
None.

Errors
- QueueAtCapacity - if the destination queue is at capacity and the contact cannot be queued within it.
- NoMatchingError - if no other Error matches.

Restrictions
This action is only supported in the customer queue flow. It is not supported in any other type of flow.

Corresponding block in the UI
Maps to Transfer to flow (p. 265) but only when used in a Customer queue flow.

TransferContactToAgent
Ends the current contact flow and transfers the customer to an agent. If the agent is already with someone else, the contact is disconnected. Transfer contact to agent works only for voice interactions.

Parameter object
No parameters are expected.

Results and conditions
None.

Errors
None.

Restrictions
This action is supported in only transfer to agent and transfer to queue flows.

Corresponding block in the UI
Transfer to agent (beta) (p. 264)

TransferContactToQueue
This action places a contact that is not already in a queue into the contact's TargetQueue. If the contact has already been put into a queue (meaning that it is currently being routed to an agent, being joined to an agent, or is connected to an agent), the action fails.

Parameter object
No parameters are expected.

Results and conditions
None.

Errors
- QueueAtCapacity - if the destination queue is at capacity and the contact cannot be queued within it.
- NoMatchingError - if no other Error matches.
Restrictions

This action is supported in contact flows and transfer flows. It is not supported in whisper flows, customer queue flows, or hold flows.

Corresponding block in the UI

Transfer to queue (p. 270)

UpdateContactAttributes

Behaving the same as the public API, this sets a collection of contact attributes. With this type of operation, either all attributes are set or none are set.

Parameter object

```
{
   "Attributes": { an Object that holds the attributes to be set.
      "Key": "Value" Both the key and value may be defined statically or dynamically.
   }
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

None. This can be used in any type of flow and any channel.

Corresponding block in the UI

Set contact attributes (p. 242)

UpdateContactCallbackNumber

Updates the contact callback number, which is the number used by the CreateCallbackContact action. This value defaults to the customer participant caller ID if this action is never used.

Parameter object

```
{
   "CallbackNumber": The callback number to set. Must be a single, valid JSONPath reference, and cannot be set statically.
}
```

Results and conditions

None.

Errors

- InvalidCallbackNumber - The callback number specified was not a valid (e.164) phone number.
- CallbackNumberNotDialable - The callback number specified is not dialable by the instance.
Restrictions

This is supported only in contact flows, transfer flows, and customer queue flows. This is not supported in whispers or hold flows.

Corresponding block in the UI

Set callback number (p. 240)

UpdateContactEventHooks

Sets one or more contact event hooks, which are flows associated with contact events, such as customer whisper or agent hold.

Parameter object

```
{
   "EventHooks": { an Object that holds the event hooks to be set. Only one entry may be present in this map.
      "Key": "Value" - the event hook to be set where the key is the event type and the value is the contact flow ID or ARN to run when that event occurs. Keys must be defined statically.
   }
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This is supported in all types of flows.

Corresponding blocks in the UI

- Set customer queue flow (p. 244)
- Set hold flow (p. 247)
- Set whisper flow (p. 253)

UpdateContactMediaStreamingBehavior

Enables or disables contact media streaming for a set of participants.

Parameter object

```
{
   "MediaStreamingState": One of "Enabled" or "Disabled". Must be specified statically.
   "Participants": [ A list of participants to include in the stream if enabling the stream, or disable if disabling the stream
       {
          "ParticipantType": The type of participant to stream. Currently, only "Customer" is supported. Must be defined statically.
       }
   ]
}
```
"MediaDirections": [ ] A list of the directions of media to include in the stream - "From" and "To". Must be defined statically.
},
"MediaStreamType": The type of media to enable or disable from the stream. Currently, only "Audio" is supported. Must be defined statically.
}

Results and conditions
None.

Errors
• NoMatchingError - if no other Error matches.

Restrictions
This is supported in contact flows, customer queue flows, transfer flows, and whisper flows. It is not supported in hold flows.

This is supported only by the voice channel.

Corresponding block in the UI
Start media streaming (p. 258) and Stop media streaming (p. 260)

UpdateContactRecordingBehavior
Sets contact recording behavior, including analysis behavior and which participants of the contact to record.

Parameter object

```
{
  "RecordingBehavior": { an object that holds the recording behavior
    "RecordedParticipants": [ ] a list of participants to record, chosen from "Agent" and "Customer". An empty list disables recording. Must be set statically.
  }
  "AnalyticsBehavior": { an object that holds the analytics behavior. Can only be set if the RecordedParticipants contains both Agent and Customer
    "Enabled": either "True" or "False". Must be set statically.
    "AnalyticsLanguage": Must be one of list of languages. Must be set statically.
    "AnalyticsRedactionBehavior": either Enabled or Disabled. Defaults to Disabled if not set. Determines whether to redact sensitive data, such as personal information, in the Contact Lens output file and audio recording.
    "AnalyticsRedactionResults": either "RedactedAndOriginal" or "RedactedOnly". Can be set dynamically. Determines whether the customer gets both the redacted and the original transcripts and audio files, or just the redacted transcripts and audio files.
  }
}
```

Results and conditions
None.

Errors
None.
Restrictions

This is supported only in contact flows, transfer flows, outbound whispers, and customer queue flows. This is not supported in agent/customer whispers or hold flows.

Analytics is only supported by the voice channel.

Corresponding block in the UI

Set recording and analytics behavior (p. 249)

UpdateContactRoutingBehavior

Updates the contact's routing details. This can move the contact forward or backward in queue, specify a queue priority, and set routing attributes.

Parameter object

```json
{
  "QueuePriority": An integer that represents the queue priority to be applied to the contact (lower priorities are routed preferentially). Cannot be specified if the QueueTimeAdjustmentSeconds or RoutingProficiencies is specified. Must be statically defined, must be larger than zero, and a valid integer value
  "QueueTimeAdjustmentSeconds": An integer that represents the queue time adjust to be applied to the contact, in seconds (longer / larger queue time are routed preferentially). Cannot be specified if the QueuePriority or RoutingProficiencies is specified. Must be statically defined and a valid integer value
  "RoutingProficiencies": { An object. Cannot be specified if either QueuePriority or QueueTimeAdjustmentSeconds is specified.
    "AgentHierarchyProficiency": { An object.
      "AgentHierarchy": The ARN of the hierarchy to preferentially route this contact to. Can be dynamic or static, but must be present.
      "ExpirationSeconds": The number of seconds after which to remove this routing proficiency. Can be dynamic or static, but must be present, and if not dynamic must be a valid integer value between 0 and 600 (inclusive).
    }
  }
}
```

Results and conditions

None.

Errors

None.

Restrictions

This is supported only in contact flows. It is not supported in transfer flows, whisper flows, customer queue flows, or hold flows.

Corresponding block in the UI

Change routing priority / age (p. 205)

UpdateContactTargetQueue

Sets the contact's TargetQueue. This is the queue is used by all other instructions that check a queue implicitly, and for TransferContactToQueue.
Parameter object

```
{
    "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be specified. This must be either defined fully statically or as a single valid JSONPath identifier.
    "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId is specified, this may not be specified. This must be either defined fully statically or as a single valid JSONPath identifier.
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported only in contact flows and transfer flows. It is not supported in whisper flows, hold flows, or customer queue flows.

Corresponding block in the UI

Set customer queue flow (p. 244)

**UpdateContactTextToSpeechVoice**

Updates the Amazon Polly voice used by text-to-speech for voice contacts (message with text-to-speech, or Amazon Lex bots). This defaults to Joanna if this action is never run.

Parameter object

```
{
    "TextToSpeechVoice": A string holding the name of an Amazon Polly voice. Must be defined statically. If this is an invalid text to speech voice, text to speech is no longer function for this contact.
    "TextToSpeechEngine": The engine associated with the Amazon Polly voice, if it is a neural voice. Must be defined statically.
}
```

Results and conditions

None.

Errors

None.

Restrictions

None. This action is supported in all flow types, and across all channels.

Corresponding block in the UI

Set voice (p. 251)
UpdatePreviousContactParticipantState

This action is primarily used to forceably prevent previous participants on the contact from observing the contact. Common use cases are disconnecting the agent that initiates a transfer when they transfer a contact to a secure destination, or putting the agent on hold when transferring to a quick connect that securely gathers customer input such as credit card numbers.

Parameter object

```json
{
    "PreviousContactParticipantState": One of ["AgentOnHold", "CustomerOnHold", "OffHold"],
    which are only supported for voice contacts.
}
```

Execution results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported only in contact flows and transfer flows.

Corresponding block in the UI

Hold customer or agent (p. 230)

Flow control actions in the Amazon Connect Flow language

These actions don’t have any side effects and are only used to determine the path through a flow. Certain data may not be available (such as contact data, if the action is determining its path based on contact data). These actions generally work in every circumstance.

A flow control action is an action that:

- Does not need a contact or a participant to succeed.
- Controls the behavior of the flow, by either enabling or disabling flow behavior (such as logging) or by choosing a branch when the flow runs.

Contents

- CheckHoursOfOperation (p. 308)
- CheckMetricData (p. 308)
- Compare (p. 309)
- DistributeByPercentage (p. 309)
- EndFlowExecution (p. 310)
- GetMetricData (p. 310)
- Loop (p. 311)
- TransferToFlow (p. 311)
- UpdateFlowLoggingBehavior (p. 312)
- Wait (p. 312)
CheckHoursOfOperation

Returns whether the specified hours of operation object (or the hours of operation object associated with the current queue if no hours of operation is referenced) is in hours or out of hours as its result, allowing comparisons against it.

Parameter object

```
{
  "HoursOfOperationId": [Optional] An hours of operation ID or hours of operation ARN.
  *Must be either fully static or fully dynamic*. If not specified, the TargetQueue's hours of operation for the contact are used
}
```

Results and conditions

True or False based on whether the hours of operation object specified is in hours or out of hours. There must be a Condition provided for Equals True and a Condition for Equals False, and no other conditions.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is available in inbound flows, transfer flows, and customer queue flows. It is not available to hold flows or to whisper flows.

Corresponding block in the UI

Check hours of operation (p. 210)

CheckMetricData

A shortcut single action to avoid using GetMetricData and Compare for a set of simple metrics. This action loads the specified metric data for the specified queue, and allows comparisons to the loaded value. For example, it loads number of contacts in queue, age of oldest contact in queue, number of agents staffed on the queue, number of agents available on the queue, or number of agents online on the queue.

Parameter object

```
{
  "MetricType": One of [NumberOfAgentsAvailable, NumberOfAgentsStaffed, NumberOfAgentsOnline, OldestContactInQueueAgeSeconds, NumberOfContactsInQueue]. **Dynamic values are not supported**,
  "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be specified. *Dynamic values are supported*,
  "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId is specified, this may not be specified. *Dynamic values are supported*. If neither this nor QueueId are specified, the contact TargetQueue is used
}
```

Execution results and conditions

A number, representing the value of the metric that was requested. This can be used for conditions. If the MetricType is NumberOfAgents* then the only supported condition is "NumberGreaterThan 0", otherwise Equals and any Number* Operands are allowed.
Errors

- NoMatchingError - if no other Error matches.
- NoMatchingCondition - if no other Condition matches (only supported if the MetricType is OldestContactInQueueAgeSeconds or NumberOfContactsInQueue).

Restrictions

This action is only usable in contact flows, queue and agent transfers, and customer queue flows. It is not available in any type of whisper or hold flows.

Corresponding block in the UI

None.

Compare

Allows comparisons against the specified value.

Parameter object

```
{
  "ComparisonValue": Any **single** JSONPath identifier that is valid for the contact flow data object
}
```

Execution results and conditions

The value specified for comparison. This can be used for conditions.

Errors

- NoMatchingCondition - if no other Condition matches.

Restrictions

This action is available in every type of flow.

Corresponding block in the UI

Check contact attributes (p. 207)

DistributeByPercentage

Returns a random number between 1 and 100 (inclusive) as its result, allowing comparisons against it.

Parameter object

```
{

}
```

Results and conditions

A number between 1 and 100, inclusive, chosen randomly. Comparisons are supported, but they must be a chain of NumericLessThan comparisons, with each subsequent comparison checking the previous value,
plus the percentage that is desired to go down this next action, and no Comparison comparing a value larger than 100.

Errors

- NoMatchingCondition if no Condition matches. This is the default option in the contact flow editor.

Restrictions

This action is available in inbound flows, transfer flows, and customer queue flows. It is not available to hold flows or to whisper flows.

Corresponding block in the UI

Distribute by percentage (p. 215)

EndFlowExecution

Finishes flow, but does not explicitly disconnect the participant. The participant may be disconnected by contact logic after this. For example, if a contact flow ends before the contact is put into queue, ending the flow results in the contact being ended.

Parameter object

```json
{
}
```

Results and conditions

None. No conditions are supported.

Errors

None. This is always a terminal action.

Restrictions

This action is available only in whisper flows and customer queue flows. It is not available in contact flows, hold flows, or transfer flows.

Corresponding block in the UI

End flow / Resume (p. 217)

GetMetricData

Loads real time queue metrics for the queue specified by queue ID, agent ID (for agent queues), or the target queue, and makes them available on the flow run data. May be extended in the future to allow getting historical metric data in addition to current metric data, and to getting agent metrics in addition to queue metrics.

Parameter object

```json
{
  "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be specified. *Dynamic values are supported*,
}
```
"AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId is specified, this may not be specified. *Dynamic values are supported*
"QueueChannel": [Optional] Either "Voice" or "Chat". Can be set dynamically. Determines the channel for which metrics are returned. If not specified, metrics are returned for all channels.

**Execution results and conditions**

None. No conditions are supported.

**Errors**

- NoMatchingError - if no other Error matches.

**Restrictions**

This action is available in every type of flow.

**Corresponding block in the UI**

Get queue metrics (p. 225)

**Loop**

When the same action (the same Action Identifier) is run multiple times, this block returns a result of "NotDone" a number of times equal to the specified loop count, then "Done" once, then reset.

**Parameter object**

```
{
  "LoopCount": Number of times to loop, must be between 0 and 100 (inclusive). Must either be fully static or fully dynamic.
}
```

**Execution results and conditions**

"ContinueLooping" if the loop should continue. "DoneLooping" if the loop should finish. Conditions are supported, there must be a Condition provided for Equals ContinueLooping and for Equals DoneLooping, and no other Conditions can be specified.

**Errors**

None.

**Restrictions**

This is supported in every type of flow.

**Corresponding block in the UI**

Loop (p. 233)

**TransferToFlow**

Execution jumps to a different flow, and continues running at that flow's beginning.
Parameter object

```
{
  "ContactFlowId": A contact flow ID or contact flow ARN. *Must be either fully static or
  a single valid JSONPath identifier*
}
```

Execution results and conditions
None.

Errors
- NoMatchingError - if no other Error matches.

Restrictions
This action is available in inbound flows and transfer flows. It is not available to hold flows, customer
queue flows, or whisper flows.

Corresponding block in the UI
Transfer to flow (p. 265)

**UpdateFlowLoggingBehavior**

Enables or disables flow logging. If this is a contact flow, this same behavior remains unless it is
overridden for the rest of the contact segment. It is also automatically inherited by new segments in the
chain.

Parameter object

```
{
  "FlowLoggingBehavior": One of [Enabled,Disabled]. *Dynamic values are not supported*
}
```

Results and conditions
None. No conditions are supported.

Errors
None.

Restrictions
This action is available in every type of flow.

Corresponding block in the UI
Set logging behavior (p. 249)

**Wait**

Pauses the flow for a specified duration, or until a specified event happens, whichever happens first.
Parameter object

```
{
  "TimeoutSeconds": The amount of time to wait before the action finishes with the
  "WaitCompleted" result. This can be either statically defined, or a single valid JSONPath
  identifier. If defined statically, this must be a positive integer value no greater than
  604800 (seven days).
  "Events": An optional list of all events that can trigger an interrupt. The only
  supported event currently is "CustomerReturned". This must be defined statically.
}
```

Execution results and conditions

If an event interrupts the wait, the run result is the event that interrupted. If no event interrupts the Wait
and the time elapses, the run result is WaitCompleted. Conditions are supported, but only the "Equals"
operator is supported. "WaitCompleted" is always required operand, and every specified event is also
required to be present as a condition operand.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This is supported in every type of flow, but is supported only by the chat channel.

Corresponding block in the UI

Wait (p. 274)

**Interactions in the Amazon Connect Flow language**

Interactions actions have side effects, but they don't require a contact or a participant. They include
actions such as invoking an AWS Lambda function. They generally work in every circumstance.

Contents

- CreateCallbackContact (p. 313)
- InvokeLambdaFunction (p. 314)

**CreateCallbackContact**

Creates a new callback contact. If no customer number is specified, and this is run in context of a contact,
the contact's CustomerCallbackNumber is used as the customer number.

Parameter object

```
{
  "QueueId": [Optional] A queue ID or queue ARN. The callback contact is routed with this
  queue, or if this is not specified, the contact's current TargetQueue. Must be specified
  fully statically or with a single valid JSONPath identifier.
  "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
  is specified, this may not be specified. This must be either defined fully statically or
  as a single valid JSONPath identifier.
  "InitialCallDelaySeconds": The amount of time, in seconds, to wait at a minimum before
  routing the callback contact. This gives the customer enough time to end their existing
  contact before being called back. Must be larger than 0, no greater than 259,200 (three
  days), and an integer. Must be defined statically.
}
```
"MaximumConnectionAttempts": The number of attempts at a maximum to connect this contact to a customer, if the callback is not answered. Must be larger than zero, and an integer. Must be defined statically.

"RetryDelaySeconds": The minimum amount of time to wait, in seconds, between an unanswered callback attempt is made and the next attempt to reach the customer. Must be larger than 0, no greater than 259,200 (three days), and an integer. Must be defined statically.

Results and conditions

None. No conditions are supported.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported in contact flows, transfer flows, and customer queue flows. It is not supported in whisper flows or hold flows.

Corresponding block in the UI

Set callback number (p. 240)

InvokeLambdaFunction

Invokes an AWS Lambda function with a collection of optional parameters. This AWS Lambda function is also given a copy of the flow run data if there is an associated contact with the flow.

Parameter object

{  "LambdaFunctionARN": The ARN of the AWS Lambda function to be invoked. May be defined statically or dynamically.
   "InvocationTimeLimitSeconds": The number of seconds to wait for a response from the AWS Lambda function. Must be greater than 0, no larger than 8, and an integer. Must be set statically.
   "LambdaInvocationAttributes" { A map of additional data to send to the AWS Lambda function when invoking it. Keys and values may be set statically or dynamically.
   }
}

Results and conditions

None. Conditions are not supported. If an error does not occur, the response's attributes are available dynamically under the $.External path.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

None. This action is supported by all channels and in all types of flows.
Corresponding block in the UI

Invoke AWS Lambda function (p. 231)

Participant actions in the Amazon Connect Flow language

Participant actions are attempted only when the flow is run in context of a participant. They generally result in an action that the participant experiences, such as playing a prompt or disconnecting.

Contents

- ConnectParticipantWithLexBot (p. 315)
- DisconnectParticipant (p. 316)
- GetParticipantInput (p. 316)
- MessageParticipant (p. 318)
- MessageParticipantIteratively (p. 318)
- TransferParticipantToThirdParty (p. 319)

ConnectParticipantWithLexBot

Connects the participant with the specified Amazon Lex bot. When the interaction is over, the Intent and Slots of the bot are available to the flow during its run.

Parameter object

```json
{
  "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along with gathering input. May not be specified if Text or SSML is also specified. Must be specified either statically or as a single valid JSONPath identifier.
  "Text": An optional string that defines text to send to the participant along with gathering input. May not be specified if PromptId or SSML is also specified. May be specified statically or dynamically.
  "SSML": An optional string that defines SSML to send to the participant along with gathering input. May not be specified if Text or PromptId is also specified. May be specified statically or dynamically.
  "LexBot": { The details of the Lex bot to invoke
    "Name": The name of the Lex bot. May be specified statically or dynamically.
    "Region": The region in which this Lex bot exists. May be specified statically or dynamically.
    "Alias": The specific alias of the Lex bot to invoke. May be specified statically or dynamically.
  },
  "LexSessionAttributes": { A map of session attributes to pass to the Amazon Lex bot when it is invoked. The keys and values may be static or dynamic.
  }
}
```

Results and conditions

If the Amazon Lex interaction succeeds, the result is the Intent of the bot. Conditions are supported, but only the Equals operator is supported within these conditions.

Errors

- NoMatchingCondition - If no specified condition evaluated to True.
- NoMatchingError - If an error occurred and no other error matched.
Restrictions

This action is supported by all channels.

This action is available only in contact flows, transfer flows, and customer queue flows. It is not available in whisper flows or hold flows.

Corresponding block in the UI

Get customer input (p. 218)

DisconnectParticipant

Disconnects the participant from the contact and stops this flow from running.

Parameter object

```
{
}
```

Results and conditions

None. Conditions are not supported.

Errors

None.

Restrictions

None. This action can be used everywhere. If there is no participant on the contact, this functions as an EndFlowExecution action, and halts the flow from running.

Corresponding block in the UI

Disconnect / hang up (p. 215)

GetParticipantInput

Gathers customer input (a DTMF collection for voice contacts, or an entered string for other channels). There are many optional behaviors after gathering this: encryption, validation, storing to a "LastParticipantInput" section on the flow run data, specifying a custom DTMF terminator for voice contacts and so on. Details are in the parameter object section.

Parameter object

```
{
    "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along with gathering input. May not be specified if Text or SSML is also specified. Must be either statically defined or a single valid JSONPath identifier.
    "Text": An optional string that defines text to send to the participant along with gathering input. May not be specified if PromptId or SSML is also specified. May be defined statically or dynamically.
    "SSML": An optional string that defines SSML to send to the participant along with gathering input. May not be specified if Text or PromptId is also specified. May be defined statically or dynamically.
    "InputTimeoutSeconds": The number of seconds to wait for input to be collected before proceeding with a timeout error. For the Voice channel this is the timeout until the
*first* DTMF digit is entered. Must be defined statically, and must be a valid integer larger than zero.

"StoreInput": "True" or "False". Must be statically defined.

"InputValidation": { An object that defines how to validate customer inputs, required if and only if StoreInput is True
  "PhoneNumberValidation": { Optional, one of the ways to validate inputs, make sure that it's a valid phone number. May not be specified if CustomValidation is specified.
    "NumberFormat": "Local" or "E164". If "Local" is specified, it is validated to be a local number (without the + and the country code), "E164" enforces that the customer input is a fully defined e.164 phone number. Must be defined statically.
    "CountryCode": If the number format is "Local", this must be defined. This is the two letter country code to be associated with the input number when validating. Must be defined statically.
  }
  "CustomValidation": { Optional, the other way to validate inputs. May not be specified if PhoneNumberValidation is specified.
    "MaximumLength": A number representing the maximum length of the input. Must be defined statically.
  }
},

"InputEncryption": { An optional object that defines how to encrypt the customer input. May only be specified if "CustomValidation" is provided.
  "EncryptionKeyId": The identifier of a key that has been uploaded in the AWS console for the purposes of customer input encryption. May be specified statically or dynamically.
  "Key": The PEM definition of the public key to use to encrypt this data. This key must be signed with the encryption key identified by the EncryptionKeyId. May be specified statically or dynamically.
},

"DTMFConfiguration": { An optional object to override default DTMF behavior for voice calls
  "InputTerminationSequence": Up to five digits to serve as the terminating sequence when gathering DTMF
  "DisableCancelKey": "True" or "False". If "True", the "*" key doesn't cancel gathering DTMF digits.
}

Results and conditions

If the "StoreInput" option is "True", there is no run result and conditions are not supported. If the "StoreInput" option is not defined or is "False", the run result is the participant input, and conditions are supported but only the Equals operator may be used on conditions. The values being compared must be static and be a single character - 0-9 numeric, *, or #.

Errors

- NoMatchingCondition - None of the specified conditions evaluated to true. Must be defined only if StoreInput is False.
- NoMatchingError - if no other Error matches. Must always be defined.
- InvalidPhoneNumber - the stored input was not a valid phone number according to the specified PhoneNumberValidation. Must be defined only if StoreInput is true, and PhoneNumberValidation is specified.

Restrictions

This action is only supported on the voice channel.

This action can be used in contact flows, transfer flows, and customer queue flows but not in whisper flows or hold flows.
Corresponding block in the UI

Get customer input (p. 218)

MessageParticipant

Sends a message to the participant. This is an audio prompt or text-to-speech for voice contacts, or a text message for other channels.

Parameter object

```
{
   "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along with gathering input. May not be specified if Text or SSML is also specified. Must be specified either statically or as a single valid JSONPath identifier.
   "Text": An optional string that defines text to send to the participant along with gathering input. May not be specified if PromptId or SSML is also specified. May be specified statically or dynamically.
   "SSML": An optional string that defines SSML to send to the participant along with gathering input. May not be specified if Text or PromptId is also specified May be specified statically or dynamically.
}
```

Results and conditions

None. No conditions are supported.

Errors

None.

Restrictions

This action is supported in contact flows, transfer flows, whisper flows, and customer queue flows. It is not supported in hold flows.

"PromptId" and "SSML" are only supported for the voice channel. All other channels support only the "Text" option.

Corresponding block in the UI

Play prompt (p. 236)

MessageParticipantIteratively

Loops a sequence of prompts while a customer or agent is on hold or in queue. This block can be configured with an interruption timeout when in a Queue flow that interrupts the message loop to run other flow logic. The message loop can include entries for both Text and Prompts.

Parameter object

```
{
   "Messages" : [ A List of messages to be played in a loop. These are defined with either TTS or a Prompt
   {
      "Text" : An optional string that defines text to send to the participant
   },
   {
      "PromptId" : A prompt ID or prompt ARN to play to the participant
   }
}
```
Results and conditions

When the timeout elapses, the action completes with the result as "MessagesInterrupted". Conditions are supported, but only the "Equals" operator is supported. The only supported operand is MessagesInterrupted.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported in Customer Queue, Customer Hold, and Agent Hold flows.

"PromptId" is supported only for the Voice channel, all other channels support only the "Text" option.

If this action is used on the chat channel, it immediately takes the error branch. If no error branch is available, the flow stop running and the contact is routed to next available agent.

Corresponding block in the UI

Loop prompts (p. 234)

TransferParticipantToThirdParty

Transfers the participant to a specified phone number. Optionally continues flow running if the third party disconnects while the participant is still connected.

Parameter object

```json
{
    "ThirdPartyPhoneNumber": A phone number, in e.164 format, of the external number to which to transfer the contact. May be defined statically or dynamically.
    "ThirdPartyConnectionTimeoutSeconds": An integer, between 0 and 600 (inclusive) representing the number of seconds to wait for the third party to answer before canceling the third party call. Only used if ContinueFlowExecution is not False. Must be defined fully statically or as a single valid JSONPath identifier.
    "ContinueFlowExecution": "True" or "False". If not defined or True, the flow continues running after the third party call finishes, if False the flow does not continue, as long as the phone call to the third party succeeds. Must be defined statically.
    "ThirdPartyDTMFDigits": An optional series of DTMF digits to send to the third party when the call succeeds. Must be defined fully statically or as a single valid JSONPath identifier. Must be 50 or fewer characters chosen from numeric digits, comma, asterisk, and pound sign.
    "CallerId": { Optional, an override of the caller ID to present when dialing the third party
        "Number": The caller ID number to present when dialing the third party. Must be defined fully statically or as a single valid JSONPath identifier.
        "Name": The caller ID name to present when dialing the third party. May be defined statically or dynamically.
    }
}
```
Results and conditions

None. Conditions are not supported.

Errors

- ConnectionTimeLimitExceeded - the call has taken longer than the specified time limit to be answered by the third party, and has been canceled. Supported only when ContinueFlowExecution is True.
- CallFailed - The call was unable to connect successfully. Only supported when ContinueFlowExecution is True.
- NoMatchingError - if no other Error matches.

Restrictions

This action is only allowed by the Voice channel.

This action is allowed in contact flows, transfer flows, and customer queue flows.

Corresponding block in the UI

Transfer to phone number (p. 267)
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.

Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list

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.

Tip
If you don't see an entry for your region, use GLOBAL. For example, there isn't an entry for ap-southeast-1, so you would use GLOBAL.

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-
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list.

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 allow list</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtc.connect-telecom.{region}.amazonaws.com</td>
<td>Replace {region} with the Region where your Amazon Connect instance is located</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>Please see the note following this table.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{myInstanceName}.a {region}.amazonaws.com/</td>
<td>Replace {myInstanceName} with the alias of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>connect/ccp-v2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{myInstanceName}.a {region}.amazonaws.com/connect/api</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>*.execute-api.</td>
<td>Replace {region} with the location of your Amazon Connect instance</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>{region}.amazonaws.com/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>participant.connect.{region}.amazonaws.com</td>
<td>Replace {region} 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 {region} 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.com</td>
<td>Replace {region} 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 allow list based on Region, see NLB endpoints (p. 324).

**Note**

The new region telecom endpoints follow a different format. Here’s a complete list of telecom endpoints:

<table>
<thead>
<tr>
<th>Region</th>
<th>Domain/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-west-2</td>
<td>rtc.connect-telecom.us-west-2.amazonaws.com</td>
</tr>
</tbody>
</table>
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list

<table>
<thead>
<tr>
<th>Region</th>
<th>Domain/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td>rtc.connect-telecom.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-central-1</td>
<td>rtc.connect-telecom.eu-central-1.amazonaws.com</td>
</tr>
<tr>
<td>ap-southeast-2</td>
<td>rtc.connect-telecom.ap-southeast-2.amazonaws.com</td>
</tr>
<tr>
<td>ap-northeast-1</td>
<td>rtc.connect-telecom.ap-northeast-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-west-2</td>
<td>rtc.cell-1.prod.eu-west-2.prod.connect.aws.a2z.com</td>
</tr>
<tr>
<td>ap-southeast-1</td>
<td>rtc.cell-1.prod.ap-southeast-1.prod.connect.aws.a2z.com</td>
</tr>
</tbody>
</table>

**Tip**
When using rtc.connect-telecom.{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 allow list instead of IP ranges:

<table>
<thead>
<tr>
<th>Region</th>
<th>CloudFront Domain</th>
</tr>
</thead>
<tbody>
<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>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://d1f0uslncc85vb.cloudfront.net/">https://d1f0uslncc85vb.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>ap-southeast-2</td>
<td><a href="https://d2190hlk727bb8.cloudfront.net/">https://d2190hlk727bb8.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://d3mgrpzmisce5.cloudfront.net/">https://d3mgrpzmisce5.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://d13tjas036gz6c.cloudfront.net/">https://d13tjas036gz6c.cloudfront.net/</a></td>
</tr>
<tr>
<td>ap-south-1</td>
<td><a href="https://d30zes7xe5707g.cloudfront.net/">https://d30zes7xe5707g.cloudfront.net/</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://dhpg19j09qxx0.cloudfront.net/">https://dhpg19j09qxx0.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>
<tr>
<td>ap-southeast-1</td>
<td><a href="https://d2g7up6vqaq2o.cloudfront.net/">https://d2g7up6vqaq2o.cloudfront.net/</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 use add these endpoints to your allow list 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>us-east-1</td>
<td>TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-central-1</td>
<td>TurnNlb-ea5316eb2759cbc.elb.eu-central-1.amazonaws.com</td>
</tr>
<tr>
<td>ap-southeast-2</td>
<td>TurnNlb-93f2de0c97c4316b.elb.ap-southeast-2.amazonaws.com</td>
</tr>
<tr>
<td>ap-northeast-1</td>
<td>TurnNlb-3c6ddabbeb821d8.elb.ap-northeast-1.amazonaws.com</td>
</tr>
<tr>
<td>eu-west-2</td>
<td>TurnNlb-1dc64a459ead57ea.elb.eu-west-2.amazonaws.com</td>
</tr>
<tr>
<td>ap-southeast-1</td>
<td>TurnNlb-261982506d86d300.elb.ap-southeast-1.amazonaws.com</td>
</tr>
</tbody>
</table>

Option 2 (not recommended): Allow IP address ranges

The second option relies on using an allow list, also known as whitelisting, the IP addresses used by Amazon Connect. You create this allow list using the IP addresses in the AWS ip-ranges.json file.

For more information about this file, see About Amazon Connect IP address ranges (p. 325).

<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>Region where your Amazon Connect instance is located (GLOBAL only if a region-specific entry doesn't exist)</td>
<td>3478 (UDP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>
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",
  "region": "GLOBAL",
  "service": "AMAZON_CONNECT"
},
```

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 allow list the ephemeral port range used by your browser, as shown in the following table.

<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>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>
</tbody>
</table>

*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.
Allow DNS resolution for softphones

If you already added Amazon Connect IP ranges to your allow list, and you don't have any restriction on DNS name resolution, then you don't need to add `TurnNlb-*.*.elb.*.amazonaws.com` to your allow list.

- To check whether there are restrictions on DNS name resolution, while on your network, use the `nslookup` command. For example:

  ```
  nslookup TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com
  ```

If you can't resolve the DNS, you must add `TurnNlb-*.*.elb.*.amazonaws.com` to your allow list.

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.*.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 allow lists 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 allow list, 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 Region where you create your instance. 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 agent 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 CTR 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 via 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.

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’s 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 via 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. 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 via 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, CTRs 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.

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 allow list 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 allow list.

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 Application integration.
4. Choose Add origin.
5. Type the URL and choose Add.
Add an Amazon Lex bot

In this article we guide you through the steps to add a 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 contact 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 created in the US East (N. Virginia) Region. After you create your instance, claim a phone number for it.

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.

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.

Create intents

For this example, you’ll configure the bot with two intents: one to look up account information, and another to speak with an agent.

1. In the Amazon Lex console choose the + icon next to Intents, and choose Create new intent.
2. Name the intent AccountLookup.
3. Create another intent, and name it SpeakToAgent.

Add sample utterances

After defining the intents, add some sample utterances.
1. Select the **AccountLookup** intent.
2. Add a sample utterance, such as *Check my account balance*, and choose the + icon.
3. 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, later in this walkthrough you’ll use numeric input to interact with a Lex bot invoked from a contact flow.

4. Select **SpeakToAgent**.
5. Add a sample utterance, such as *Speak to an agent*, and choose +.
6. Add a second utterance, such as *Two*, and choose +.

### Add slots

Before the bot can respond with the caller’s account balance, it needs the account number.

1. Choose the **AccountLookup** intent.
2. Under **Slots**, add a slot named **AccountNumber**.

3. For **Slot type**, use the drop-down to choose **AMAZON.NUMBER**.
4. 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.*
5. Choose the + icon.
6. Make sure that the **Required** check box is selected.

### Add responses

Now that you have intents, utterances, and a slot, add the responses that the bot provides to callers. Because you are creating a simple bot for this example, you are not hooking up the bot to look up real customer data. The example bot responds with text strings that you add, regardless of the account number that a caller provides.
1. Select the **AccountLookup** intent.
2. In the **Response** section, add a message for the bot to say to customers. For example, “The balance for your account is $2,586.34.”
3. Choose **Save Intent**.
4. For the **SpeakToAgent** intent, 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.”
5. Choose **Save Intent**.

---

### Build and test the Amazon Lex bot

After you create your bot, make sure it works as intended before you publish it.

1. Choose **Build**. It may take a minute or two.
2. When it’s finished building, choose **Test Chatbot**.

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.
4. Choose Clear chat history.
5. To confirm that the SpeakToAgent intent is working, type 2.

Publish the Amazon Lex bot and create an alias

Next, publish the bot so that you can add it to a contact flow in Amazon Connect.

1. Choose Publish.
2. Provide an alias for your bot. Use the alias to specify this version of the bot in the contact flow, for example, Test.
   
   **Important**
   
   In a production environment, always use a different alias than $LATEST. Only use $LATEST for manual testing. If the bot alias is $LATEST Lex invocations are throttled. For more information, see Runtime Service Quotas.
3. Choose Publish.

Add the Amazon Lex bot to an Amazon Connect instance

Before you can use a bot in your contact flow you need to add it to your Amazon Connect instance. You can only add bots created under the same AWS account.

If you add Amazon Lex bots created in a different Region from your instance, performance may be affected.

1. Open the Amazon Connect console.
2. Select the Instance Alias of the instance to which to add the bot.
3. Choose Contact flows.
4. Under Amazon Lex, use the drop-down to choose a name for your bot and then choose + Add Lex Bot.
5. Select the AccountBalance bot and choose Save Lex Bots. If the name of your bot doesn't appear in the list, reload the page to get it to show up.

Create a contact flow and add your Amazon Lex bot

Next, create a new contact flow that uses your Amazon Lex bot. When you create the contact 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.
2. Choose Routing, Contact flows, Create contact flow, and type a name for the flow.
3. Under Interact, drag a Get customer input (p. 218) block onto the designer, and connect it to the Entry point block.
4. Click the **Get customer input** block to open it. Choose **Text to speech (Ad hoc), 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.”

---

**Add the Amazon Lex bot to your contact flow**

In this step you’ll specify the bot as the method of getting customer input.

1. In the **Get customer input (p. 218)** block select **Amazon Lex**.
2. For **Name**, use **AccountBalance**. For **Alias**, use **Test**.

**Important**

In a production environment, always use a different alias than $LATEST. Only use $LATEST for manual testing. If the bot alias is $LATEST Lex invocations are throttled. For more information, see Runtime Service Quotas.
3. Under **Intents**, choose **Add an intent**.
4. Type **AccountLookup** and choose **Add another intent**.

5. Type **SpeakToAgent** and choose **Save**.

**Finish the contact flow**

After the caller interacts with the bot, finish the contact flow to complete the call for the customer.

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 contact flow.

To complete the **AccountLookup** intent:

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/hang up 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 customer 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 block to the Transfer queue.
4. Choose Save, then Publish.

Your finished contact flow will look something like the following one:

![Contact Flow Diagram](image)

Assign the contact flow to a phone number

When callers call in to your contact center, the contact flow to which they are sent is the one assigned to the telephone number that they dialed. To make the new contact flow active, assign it to a phone number for your instance.

1. Open the Amazon Connect Dashboard.
2. Choose View phone numbers.
3. Select the phone number to which to assign the contact flow.
4. Add a description.
5. In the Contact flow/IVR menu, choose the contact flow that you just created.
6. Choose Save.

Try it!

To try the bot and contact flow, call the number you assigned to the contact flow. Follow the prompts.
Invoke AWS Lambda functions

Amazon Connect can interact with your own systems and take different paths in contact flows dynamically. To achieve this, invoke AWS Lambda functions in a contact 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.

To invoke a Lambda function from a contact flow, complete the following tasks.

Tasks
• Create a Lambda function (p. 339)
• Add a Lambda function to your Amazon Connect instance (p. 339)
• Invoke a Lambda Function from a Contact Flow (p. 340)
• Configure your Lambda function to parse the event (p. 342)
• Verify the function response (p. 342)
• Consume the Lambda function response (p. 343)

Create a Lambda function

Create a Lambda function, using any runtime, and configure it. For more information, see Create a Lambda Function 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 (p. 339). 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 contact flow using the contact 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 contact 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. Choose the name of the instance from the Instance Alias column.
3. In the navigation pane, choose **Contact 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.

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 contact flows.

---

**Invoke a Lambda Function from a Contact Flow**

To view a contact flow that invokes a Lambda function, see Sample Lambda integration (p. 168).

1. Open or create a contact flow.
2. Add an **Invoke AWS Lambda function** (p. 231) 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** (p. 231) 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. This creates a branch for you to specify what to do if it times out.

For every Lambda function invocation from a contact 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": {},
            "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-XXXXXXXXXX",
            "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "Queue": {
                "ARN": "arn:aws:connect:eu-west-2:11111111111:instance/ccccc-cbbbd-ddd-
eee-fffffffffff/queue/aaaaa-bbbcccc-ddd-eereeeeeeeeee",
                "Name": "PasswordReset"
            },
            "SystemEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            }
        },
        "Parameters": {
            "sentAttributeKey": "sentAttributeValue"
        }
    },
    "Name": "ContactFlowEvent"
}
```

The request is divided into three parts:

- **Contact data**—This is always passed by Amazon Connect for every contact. Some parameters are optional.
- **User attributes**—These are attributes that have been previously associated with a contact, such as when using a Set contact attributes block in a contact flow. This map may be empty if there aren't any saved attributes.
- **Parameters**—These are parameters specific to this call that were defined when you created the Lambda function.
Invocation retry policy

If your Lambda invocation in a contact 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

Amazon Connect limits the duration of a sequence of Lambda functions to 20 seconds. It will error out when the total execution time exceeds this threshold. Since customers hear silence while a Lambda function executes, we recommend adding a Play prompt block between functions to keep them engaged and aware of the long interaction.

By breaking up a chain of Lambda functions with the Play prompt block, you will be able invoke multiple functions that last longer than the 20 second threshold.

Configure your Lambda function to parse the event

To successfully pass attributes between your Lambda function and Amazon Connect, configure your function to correctly parse the JSON request sent from the Invoke AWS Lambda function block, 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 example shows how to access sentAttributeKey using Node.JS:

```javascript
var receivedAttribute = event['Details']['Parameters']['sentAttributeKey'];
```

Verify the function response

The Lambda function response should be a simple string map. This map can be up to 32k. 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 contact 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) {

var resultMap = {
    Name: 'CustomerName',
    Address: '1234 Main Road',
    CallerType: 'Patient'
}

callback(null, resultMap);
}
```

This example shows an example response using Python:
Consume the Lambda function response

There are two ways to use the function response in your contact 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.

Access variables directly

If you access the variables directly, you can use them in contact flow blocks, but they are not included in contact trace records (CTR). To access these variables directly in a contact 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

Make sure that the name specified for the source attribute matches the key name returned from Lambda.

Store variables as contact attributes

If you store the variables as contact attributes, you can use them throughout your contact flow, and they are included in CTRs.

To store the values returned as contact attributes and then reference them, use a Set contact attributes block in your contact flow after the Invoke AWS Lambda function block. Choose External for the Type. Following the example we're using, set Destination key to returnedContactName, and set the Source attribute to Name.

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.

Make sure that the name specified for the source attribute matches the key name returned from Lambda.
Encrypt customer input

You can encrypt sensitive data that is collected by contact flows. To do this, you need to use public-key cryptography. Here’s how this works:

Amazon Connect requires an X.509 certificate that is signed using the same private key that will decrypt data.

In a contact 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 contact flow.

Note
You can have up to two signing 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.

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";
}
```
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 contact 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 contact flow
    String cypherText = args[2]; // the result from contact 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);
    RSAPrivateKey privKey = (RSAPrivateKey) kf.generatePrivate(keySpec);
    return privKey;
}
Capture customer audio: live media streaming

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 contact 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 (p. 346)
- Enable live media streaming in your instance (p. 347)
- How to access Kinesis Video Streams data (p. 348)
- Example contact flow for testing live media streaming (p. 353)
- Contact attributes for live media streaming (p. 354)

Plan for live media streaming

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.

Check out the default Kinesis service quota for number of streams per account for your region (see the quota for the CreateStream API).

To make sure that there are enough streams available for all calls in your contact center, the value of the CreateStream API needs to be greater than the number of the maximum concurrent active calls for your instance.
If you have more than one instance for your AWS account, your `CreateStream` quota should be a number greater than the concurrent active calls for all of your instances combined.

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 (p. 347)`.

**Tip**
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.

### 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 policies and permissions, the IAM 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/](https://console.aws.amazon.com/connect/).
2. Choose the instance alias for the instance from the `Instance Alias` column.
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 master key to use to encrypt the data sent to Kinesis.
7. Specify a number and unit for the `Data retention period`. If you select `No data retention`, data is not retained and can be used only for immediate consumption.
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 contact flow. Configure those blocks to specify what audio you want to capture. For instructions and an example, see `Example contact flow for testing live media streaming (p. 353)`.

---

347
How to access Kinesis Video Streams data

You must have developer skills to work with Kinesis Video Streams data. Use the steps and code samples in this section to interact with the customer audio data sent to Kinesis Video Streams.

Get started with a sample

There's an example project on GitHub to help you to get started using Amazon Connect live audio streaming and real-time transcription using Amazon Transcribe. See Amazon Connect Real-time Transcription Lambda.

This project provides a code example and a fully functional Lambda function. They help you get started capturing and transcribing Amazon Connect phone calls using Kinesis Video Streams and Amazon Transcribe.

You can use the Lambda function in this project to create other solutions, such as:

• Capturing audio in the IVR.
• Providing real-time transcription to agents.
• Creating a voicemail solution for Amazon Connect.

Build your own implementation

You may want to implement a solution other than the one provided by the previously-described sample. If so, this section describes how to make the proper API calls against the Kinesis Video Streams so you can build your own solution from scratch.

1. Go to this GitHub page, and read about the Amazon Connect Real-time Transcription Lambda project.
2. Choose the deployment folder, and download the cloudformation.template.
3. Use the following example Java classes, which are built on top of the Kinesis video parser library using the AWS SDK for Java.

   • LMSDemo—is a class with a main method that invokes LMSExample.
   • LMSExample—is similar to the examples provided in the Kinesis Video Streams Parser library. It gets media from the specified Kinesis Video Streams with the specified fragment number. This code sample includes frame processing to separate the tracks.
   • LMSFrameProcessor—is invoked by LMSExample to save data from Kinesis Video Streams to the specified output stream. Use a file output stream to save the output to a file. This code sample also includes frame processing to separate the tracks.
4. Use Audacity, or other audio tool, to import the .raw audio file, which is in a 16-bit signed PCM Mono format.

Code samples to access Kinesis Video Streams data

LMSDemo.java

```java
package com.amazonaws.kinesisvideo.parser.demo;

import com.amazonaws.auth.AWSProfileCredentials;
import com.amazonaws.auth.AWSProfileCredentialsProvider;
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>>";
                        }
                    };
                }
            },
            new FileOutputStream("<<FileName>>.raw");
        example.execute();
    }
}

LMSExample.java

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;

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;

        public LogVisitor(FragmentMetadataVisitor fragmentMetadataVisitor) {
            this.fragmentMetadataVisitor = fragmentMetadataVisitor;
        }

        public void visit(MkvElement element) {
            fragmentMetadataVisitor.visit(element);
        }
    }
}
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");
    }
}

@Override
public void visit(MkvDataElement dataElement) throws MkvElementVisitException {
}

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 {
    
}
}

LMSFrameProcessor.java

package com.amazonaws.kinesisvideo.parser.utilities;

import com.amazonaws.kinesisvideo.parser.mkv.Frame;
import com.amazonaws.kinesisvideo.parser.utilities.FragmentMetadataVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.MkvTrackMetadata;
import java.io.IOException;
import java.io.OutputStream;
import java.nio.ByteBuffer;

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;
        this.fragmentMetadataVisitor = fragmentMetadataVisitor;
    }

    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_FROM_CUSTOMER".equals(trackName)) {
                outputStreamToCustomer.write(frameBytes);
            } else {
                // Unknown track name. Not writing to output stream.
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
Example contact flow for testing live media streaming

Here's how you can set up a contact 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 contact flow.

Use the contact attributes for media streaming in your contact flow so that the CTR includes the attributes. You can then view the CTR 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 contact flow shows how you might use media streaming with attributes for testing purposes.
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** (p. 354).

Contact attributes for live media streaming

The attributes are displayed when you select **Media streams** for the **Type** in a contact 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.

  **JSONPath format:** `.MediaStreams.Customer.Audio.StreamARN`

- **Customer audio start timestamp**
  
  The time at which the customer audio stream started.

  **JSONPath format:** `.MediaStreams.Customer.Audio.StartTimestamp`

- **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.StartPosition`
Customer audio stop fragment number

The number that identifies the Kinesis Video Streams fragment in which the customer audio stream stopped.


For more information about Amazon Kinesis Video Streams fragments, see Fragment in the Amazon Kinesis Video Streams Developer Guide.
Integrate with your CRM

You can integrate Amazon Connect with your customer relationship management (CRM) application. Integration allows you to launch your contact center in your CRM of choice, maintain your existing user base, and use the Amazon Connect cloud-based infrastructure.

To integrate the Contact Control Panel (CCP) into your CRM, see Amazon Connect Streams. When completed, add the origin URLs to your instance settings. This enables communication between Amazon Connect and your CRM. For more information, see Use an allow list for integrated applications (p. 331).

Contents

- Amazon Connect and Salesforce integration (p. 356)
- Amazon Connect and Zendesk integration (p. 356)

Amazon Connect and Salesforce integration

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 v5 for Salesforce Lightning installation guide.

For the CTI Adapter for Salesforce Classic, see the Amazon Connect CTI Adapter v5 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.

Amazon Connect and Zendesk integration

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 contact flows to use Amazon Connect with Zendesk ticketing.

For more information, see How do I integrate Amazon Connect with Zendesk?
Manage users in Amazon Connect

As the admin one of your key responsibilities will be to manager 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.

Contents

• Add users to Amazon Connect (p. 357)
• Delete users from your Amazon Connect instance (p. 358)
• Reset a user’s password for Amazon Connect (p. 360)
• Security profiles (p. 361)

Add users to Amazon Connect

You can add users and configure them with permissions that are appropriate to their roles (for example, agents or managers). For more information, see Security profiles (p. 361). Contacts can be routed based on the skills required of the agents. For more information, see Create a routing profile (p. 126).

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.

![Permission Table]

By default, the Amazon Connect Admin security profile has these permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 366).

Add a user individually

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 users.
2. 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, and password for the user.
6. Choose a routing profile and a security profile.
7. 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.

8. For information about adding agents, see Configure agent settings: routing profile, phone type, and auto-accept calls (p. 131).

Add users in bulk from a csv file

Use these steps to add several users from a csv file such as an Excel spreadsheet

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 users.
2. Choose Users, User management.
3. Choose Add new users.
4. Choose Upload my users from a template (csv) and then choose Next.
5. Choose Download template.
6. Add your users to the template and upload it to Amazon Connect.

If you get an error message, it usually indicates that one of the required columns is missing information, or there's a typo in one of the cells.

• We recommend checking the format of the phone number as a starting point in your investigation.
• If you get an error message that Security profile is not found, check whether there's a typo in one of the cells in the security_profile_name_1 column.
• Update the .csv file and try uploading it again.

Delete users from your Amazon Connect instance

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.

What happens to the user's metrics?

The user's data in CTRs and reports is retained. The data is preserved for the consistency of the historical metrics.
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.

**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.

**How to delete users**

You can't undo a deletion.

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to remove users.
2. Choose the user account you want to delete, and then choose Remove.
3. Confirm you want to delete that account.
To reset a password for a user

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. 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 (p. 92).

Reset your 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 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 (p. 361)
- About inherited permissions (p. 362)
- Default security profiles (p. 364)
- Assign a security profile to a user (p. 364)
- Create a security profile (p. 365)
- Update security profiles (p. 366)

**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.
- Change the login credentials of a user, including the login username.
- 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** (p. 502) 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 (p. 362)

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.

- Track who accesses recordings (p. 373).

In the **Metrics and quality** permission group, you can enable a download icon for recorded conversations. When members of this group go to **Metrics and quality**, **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 table](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 phone numbers and hours of operation appear in the drop-down 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.

**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>
</table>
| Users - View or Edit | When someone edits a user's information in the Amazon Connect console, they can view the following information in drop-down boxes when they add it to the user's account:  
  - All security profiles in the instance  
  - All routing profiles in the instance  
  - All agent hierarchies in the instance |
| Queues - View or Edit | When someone edits queues in the Amazon Connect console, they can view the following information in drop-down and search boxes when they add it to the queue:  
  - All quick connects in the instance  
  - All phone numbers in the instance  
  - All operating hours in the instance |
### 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 all 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>

### 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. 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](#) (p. 361).
2. Log in to your contact center using your access URL (https://instance name.awsapps.com/connect/login).
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 the following permissions: Security profiles - Create.

![Users and permissions](#)

By default, the Amazon Connect Admin security profile has these permissions.

**How to create security profiles**

1. Log in to your contact center using your access URL (https://instance name.awsapps.com/connect/login).
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**.

### 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**.

By default, the Amazon Connect **Admin** security profile has these permissions.

### How to update security profiles

1. Log in to your contact center using your access URL (https://instance name.awsapps.com/connect/login). You must be logged in with an Amazon Connect account that has permissions to update security profiles.
2. Choose **Users**, **Security profiles**.
3. Select the name of the profile.
4. Update the name, description, and permissions as needed.
5. Choose **Save**.
Monitor live and recorded conversations

The articles in this section explain how to monitor (listen-in) on conversations between agents and contacts.

Contents
- Monitor live conversations (p. 367)
- Review recorded conversations (p. 370)

Monitor live conversations

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 contact 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 Feature specifications (p. 568).

Set up live monitoring for voice and/or chat

1. Add the Set recording and analytics behavior (p. 249) block to your contact flow. Do this to monitor calls, chats, or both.

   To enable monitoring of voice and/or chat conversations, in the block's properties choose Agent and Customer.
## Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

### Call recording

Enables or disables call recording for the agent, customer, or both. Agent and customer call recordings are required to enable Contact Lens.

<table>
<thead>
<tr>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
</tr>
<tr>
<td>Agent and Customer</td>
</tr>
<tr>
<td>Agent only</td>
</tr>
<tr>
<td>Customer only</td>
</tr>
<tr>
<td>Off</td>
</tr>
</tbody>
</table>

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 contact 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, remove the Amazon S3 buckets. For instructions, see [Update instance settings](#).

### 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.
Monitor conversations

4. Choose Save.

To create a new security profile for monitoring live conversations

2. Choose Add new security profile.
3. Expand Metrics and Quality, then choose Access metrics and Manager monitor.

<table>
<thead>
<tr>
<th>Metrics and Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Access metrics</td>
</tr>
<tr>
<td>Contact search</td>
</tr>
<tr>
<td>Contact attributes</td>
</tr>
<tr>
<td>Login/Logout report</td>
</tr>
<tr>
<td>Manager monitor</td>
</tr>
<tr>
<td>Recorded conversations</td>
</tr>
<tr>
<td>Saved reports</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Contact Control Panel (CCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Access Contact Control Panel</td>
</tr>
<tr>
<td>Make outbound calls</td>
</tr>
</tbody>
</table>

These permissions are needed so they can monitor the conversation through the Contact Control Panel.

5. Choose Save.

Monitor live conversations with contacts

Tip
Call barge-in is not currently supported. That is, if you're listening to a conversation, your microphone stays muted.

1. Check that the Set recording and analytics behavior (p. 249) block is in the contact flow you want to monitor. It has to be there whether you're monitoring calls or chats. In the block's Properties, choose Agent and Customer.
2. Log in to your Amazon Connect instance with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Manager monitor permission.
3. 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.

4. To choose the agent conversation you want to monitor, in Amazon Connect choose **Metrics and quality, Real-time metrics, Agents.**

5. To monitor voice conversations: Next to the names of agents in a live voice conversation, you’ll see a headset icon. Choose the icon to start monitoring the conversation.

   When you’re monitoring a conversation, the status in your CCP changes to **Monitoring.**

6. 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.**

7. To stop monitoring the conversation, in the CCP choose **End call** or **End chat.**

   When the agent ends the conversation, monitoring stops automatically.

### Review recorded conversations

Managers can review past conversations between agents and customers. To set this up, you need to **set up recording behavior** (p. 190), 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. If the call is transferred externally, the call recording stops when the agent drops from the call.

**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 trace record (CTR) (p. 469). The recording is available in the CTR, however, only after the contact has left the After Contact Work (ACW) state (p. 414).

### Assign permissions to review recordings of past conversations

**To assign a manager permissions to review recordings of past conversations**

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. If you also want the manager to monitor live conversations, assign the manager to the **Agent** security profile so they can access the Contact Control Panel (CCP). This is so they can monitor the conversation through the CCP.

4. For the manager to listen to recordings that have been redacted, assign **Recorded conversations (redacted)** permissions to the security profile. For more information about these permissions, see **Security profile permissions for Contact Lens** (p. 383).

   The redaction feature is provided as part of Contact Lens for Amazon Connect. For more information, see **About sensitive data redaction in Contact Lens** (p. 394).

5. Choose **Save.**
Or, to create a new security profile specific for this purpose

2. Choose Add new security profile.
3. Expand Metrics and Quality, then choose Manager monitor and Recorded conversations (choose both Access and Enable download button).
4. If you also want the manager to monitor live conversations, assign the manager to the Agent security profile so they can access the Contact Control Panel (CCP). This is so they can monitor the conversation through the CCP.
5. For the manager to listen to recordings that have been redacted, assign Recorded conversations (redacted) permissions to the security profile. For more information about these permissions, see Security profile permissions for Contact Lens (p. 383).
6. Choose Save.

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 (p. 370).
2. In Amazon Connect choose Metrics and quality, 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.
   ![Sample chat transcript](image)
5. To listen to a recording of a voice conversation, or read the transcript of a chat, choose the Play icon.
6. The following image shows a sample chat transcript.
Download recordings/transcripts of past conversations

These are the steps that a manager does to download past recordings/transcripts of conversations.

1. Log in to Amazon Connect with a user account that has permissions to access recordings (p. 370).
2. In Amazon Connect choose Metrics and quality, 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.
5. Choose the Download icon.
6. The recording is saved automatically to your Downloads folder as a .wav file.
Track who deleted or listened to recordings

You need an AWS account to do these steps.

Set up logging

1. If you have multiple instances and buckets, look up the name of the Amazon S3 bucket for your instance. Go to the Amazon Connect console, choose the instance alias, and choose Data storage.

2. Go to the Amazon S3 console.
3. Choose the Amazon S3 bucket where your recordings are stored.

4. Choose the Properties tab.
5. Choose Object-level logging and then choose View CloudTrail trails.

It opens the AWS CloudTrail console.
6. In the navigation menu, choose Trails and then choose the trail name.
7. In the upper right corner, toggle **Logging** to **ON**, if it’s not on already.

8. Under **Management** events, choose the edit icon. To log only who deletes recordings, you set this to **Write-only**. To also log who listens to recordings, set to **All**. Choose **Save**.

9. Under **CloudWatch Logs** choose the edit icon. Either accept the default name for your log group (*CloudTrail/DefaultLogGroup*), or specify a new name. Choose **Continue**.

10. Choose **Allow**. You can now close the AWS CloudTrail console.

**Find who deleted or listened to recordings**

1. Go to the Amazon CloudWatch console.
2. Choose **Create dashboard**.
3. Enter a name, such as **CloudTrail-logging**.

4. On the **Add to this dashboard** dialog box, choose **Query results**. Choose **Configure**.

5. In the **Select log groups**, use the drop-down arrow to choose the log group for your instance, such as **CloudTrail/DefaultLogGroup**.

6. In the query box, delete the current query, and then copy and paste the one shown below instead. This query will find all API events where the recording was deleted:

```sql
fields @timestamp, @message
| filter eventSource = 's3.amazonaws.com'
| filter eventName = 'DeleteObject'
```

7. In the time box, choose how far back you want to search.

8. Choose **Run query**.

   It returns all of the events that are named **DeleteObject**.

9. Next to the event, choose the arrow. It expands to show you detailed information about the event, including the ID of the user who deleted the recording.

10. If a lot of records are returned, choose the **Actions** arrow, and then choose **Download query results (CSV)**. The data is exported to Excel. From there you can format the spreadsheet so it's easier for you to search and see the names of the users who deleted recordings.

   The following image shows what the @message column looks like in the CSV file.
11. If you're also logging who listened to recordings, update the query to search for the `eventName` `GetBucketLocation`.

```sql
fields @timestamp, @message
| filter eventSource = 's3.amazonaws.com'
| filter eventName = 'GetBucketLocation'
```

**Tips**

Mirroring CloudTrail logs to CloudWatch is useful but optional. Mirroring the CloudWatch log allows you to use CloudWatch Insight to search the events easily.

If you have a large contact center, you may not want to use object logging because it generates many logs that are stored in your Amazon S3 bucket.

Another option is to write an AWS Lambda function to process the CloudTrail events. You can also search the logs manually.

**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.

1. Log in to Amazon Connect with a user account that has permissions to access recordings (p. 370).
2. In Amazon Connect choose Metrics and quality, Contact search.
3. In the Contact ID, enter the contact ID, and then 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.
To learn more about searching, see Search for contacts (p. 467).
Analyze conversations using Contact Lens for Amazon Connect

Contact Lens for Amazon Connect lets you analyze customer-agent conversations, by using speech transcription, natural language processing, and intelligent search capabilities. It performs sentiment analysis and automatically indexes call transcripts so that you can search for specific words/phrases. This enables supervisors to identify recurring themes, and discover opportunities to coach agents so that they can continually improve the customer experience.

The results of the sentiment analysis appear in the customer’s Contact Trace Record (CTR). The following image shows a portion of a CTR with sentiment analysis.

Contents
- Enable Contact Lens for Amazon Connect (p. 378)
- Security profile permissions for Contact Lens (p. 383)
- Automatically categorize contacts based on uttered keywords and phrases (p. 385)
- Search conversations analyzed by Contact Lens (p. 388)
- Review analyzed conversations using Contact Lens (p. 391)
- About sentiment scores and non-talk time in Contact Lens (p. 393)
- About issue/call driver detection in Contact Lens (p. 393)
- About loudness scores in Contact Lens (p. 394)
- About sensitive data redaction in Contact Lens (p. 394)
- Example Contact Lens output files (p. 395)
- Error notifications: When Contact Lens can’t analyze a contact (p. 404)

Enable Contact Lens for Amazon Connect

To enable Contact Lens in a contact flow, add a Set recording and analytics behavior (p. 249) block for the flow, and configure it for Contact Lens.
Tip
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 (p. 249) block with Enable analytics enabled for the flow. This is because a transfer generates a second contact ID and CTR. Contact Lens needs to run on that CTR as well.

To enable Contact Lens in a contact flow

1. Add the Set recording and analytics behavior (p. 249) block to a contact flow.
2. In the contact block, under Call recording, choose On, Agent and Customer. You need both agent and customer call recordings to use Content Lens.

   Set recording and analytics behavior

   Specify call recording behavior and configure Contact Lens speech analytics.

   Call recording

   Enables or disables call recording for the agent, customer, or both. Agent and customer call recordings are required to enable Contact Lens.

   On
   Agent and Customer
   Agent only
   Customer only
   Off

3. Select Enable Contact Lens for speech analytics.
4. Choose the language.

5. Choose Save.

6. If the contact is going to be transferred to another agent or queue, repeat these steps to add another Set recording and analytics behavior (p. 249) block with Enable Contact Lens for speech analytics enabled.

How to enable redaction of sensitive data

To enable redaction of sensitive data in a contact flow, choose Redact sensitive data.

- Redact sensitive data

Redact sensitive data, such as personal information, in the Contact Lens output file and get a redacted audio recording. Sensitive data redaction is currently available for certain languages only. Learn more

- Get redacted and original transcripts, and redacted audio

- Get redacted transcript and audio only

- Use attribute
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 Example Contact Lens output files (p. 395).

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 (case sensitive)
  - None
  - RedactedOnly
  - RedactedandOriginal
- Language: choose one of the following (case sensitive)
  - en-US
  - en-GB
  - en-IN
  - en-AU
  - es-US: Redaction is not supported for this language

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 Using a Set contact attributes block (p. 279). Define the Destination key and Value for redaction and language as needed.

  The following image shows how to use contact attributes for redaction:
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:

- Use text
  - Destination key
    - language
  - Value
    - en-US
- Use attribute

This is case sensitive!
**Use a Lambda function** (p. 279). This is similar to how you set up user-defined contact attributes. A 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'
}
```

---

**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 security profile permissions shown in the following image apply to Contact Lens.

Following is a description of each of these 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 Contact Lens functionality appears.
Search contacts by conversation characteristics

On the Contact Search page, you can access additional filters that allow you to return results by sentiment score and non-talk time. For more information, see Search conversations analyzed by Contact Lens (p. 388).

Search contacts by keywords

On the Contact Search page, you can access additional filters that allow you to search call transcripts by keywords or phrases, such as “thank you for your business.” For more information, see Search conversations analyzed by Contact Lens (p. 388).

Contact Lens - speech analytics

On the Contact Trace Record page for a contact, you can view graphs that summarize speech analytics: customer sentiment trend, sentiment, and talk time. For example, the following image shows how this information is displays on the CTR page for a contact.

Rules

This permission allows you to view, edit, or create rules for categorizing contacts. For more information, see Automatically categorize contacts based on uttered keywords and phrases (p. 385).

Recorded conversations (redacted)

On the Contact Trace Record page for a contact, this permission allows you to listen to call recording files and view call transcripts in which the sensitive data has been removed. For more information, see Example redacted file (p. 400).

Recorded conversations (unredacted)

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 transcripts
- Original, unredacted transcripts analyzed by Contact Lens
- Original, unredacted audio recordings

You can access this content on the Contact Trace Record page for a contact. For more information, see Example original, analyzed file (p. 395).

Important

If you have permissions to both Recorded conversations (redacted) and Recorded conversations (unredacted), by default only redacted recordings are made available on the Contact Trace Records page. You must remove permissions to Recorded conversations (redacted) to access unredacted conversations. You can’t access redacted and unredacted content at the same time.
Automatically categorize contacts based on uttered keywords and phrases

You can set up Contact Lens to analyze conversations for certain words or phrases, and then highlight where they are uttered in the conversation. This is useful to do when, for example, you want to ensure that agents are speaking certain words or phrases 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, you add rules that contain the word or phrases you want to highlight.

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 Rules permissions. For more information, see Security profile permissions for Contact Lens (p. 383).

How to add rules

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 choose Metrics and quality, Rules.
3. Assign a name to the rule.
4. Enter the words or phrases, separated by a comma, that you want to highlight.
5. 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: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business), etc.

6. 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.
The logic that Contact Lens uses to read the two groups of words or phrases is (group 1) AND (group 2).

7. When done, choose **Save**.

8. After you add the rules, they are applied in real time to **new** contacts when Contact Lens analyzes conversations. You can't analyze past, stored conversations.

### Tips for adding rules

Following are some tips for adding rules:

- It's an exact word match, singular or plural.
- AND OR are allowed.
- To enter a script, 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.

### Rules are applied to new contacts

After you add the rules, they are applied in real time to **new** contacts when Contact Lens analyzes conversations. You can't analyze past, stored conversations.
Search conversations analyzed by Contact Lens

After a call ends and the agent completes After Contact Work (ACW), Contact Lens analyzes and transcribes the recording of the customer-agent conversation.

You can search the analyzed and transcribed recordings based on:

- Speaker.
- Keywords.
- Sentiment score.
- Non-talk time.

These criteria are described in the following sections.

Required permissions for searching conversations

Before you can search conversations, you need the following permissions, which allow you to do the type of search you want.

- **Contact search**. This is required so you can get to the Contact Search page.
- **Search contacts by conversation characteristics**
- **Search contacts by keywords**

For more information, see Security profile permissions for Contact Lens (p. 383).

Search for keywords

For search, Contact Lens uses the standard analyzer in Amazon Elasticsearch 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 keywords

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 **Metrics and quality**, **Contact search**.
3. In the **Filter** section, specify the time period that you want to search. Include other information to narrow your search. For instructions, see Search for contacts (p. 467).
   
   **Tip**
   
   When searching by date, you can search up to 14 days at a time.
4. In the **Conversation** 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.

   - 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").

<table>
<thead>
<tr>
<th>Words or phrases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words or phrases</td>
</tr>
<tr>
<td>hello, cancellation, &quot;example airline&quot;</td>
</tr>
</tbody>
</table>

- 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").

<table>
<thead>
<tr>
<th>Words or phrases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words or phrases</td>
</tr>
<tr>
<td>&quot;thank you for your business&quot;, cancellation, &quot;example airline&quot;</td>
</tr>
</tbody>
</table>

**Search for sentiment score or evaluate sentiment shift**

With Contact Lens, you can search conversations for sentiment scores 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 calls where the customer sentiment ended negatively. You might search for all calls where the sentiment score is <= (less than or equal to) -4.

**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 for the entire contact**: This returns the average score for the customer or agent's portion of the conversation.
   - **Evaluating sentiment shift**: Identify where the customer or agent's sentiment changed during the contact.

   For example, you might search where the customer's sentiment score begins at less than or equal to -1 and ends at greater than or equal to +1.
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.
Review analyzed conversations using Contact Lens

By using Contact Lens for Amazon Connect, you can review the transcript and identify what part of the call is of interest. You won't need to listen to an entire call to find out what's interesting about it.

For example, you might scan the transcript of the call and see a red sentiment emoji for a customer turn. You can choose the timestamp and jump to that portion of audio recording.

Review an analysis of a voice conversation

1. Log in to Amazon Connect with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Contact search and Contact Lens - speech analytics permissions.
2. In Amazon Connect, choose Metrics and quality, 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 (p. 467).
4. Choose the contact ID to view the Contact Trace Record (CTR) for the contact.
5. In the Recording and transcript section of the CTR, review what was spoken and when, and their sentiment.
6. If desired, choose the play prompt to listen to the recording. Or, download the recording and fast-forward to only the portion you're interested in.
Turn-by-turn transcript

Busy supervisors often need to review a lot of calls. 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.

Following are key features of the turn-by-turn transcript:

Auto scroll

The audio recording and transcript are in sync. You can quickly scroll through the transcript, stop at interesting turns, and choose the timestamp for the turn to listen that specific point in the recording.

Sentiment emojis

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 recording to hear how that agent helped the customer.

Issue detection

Issues (also known as call drivers) are turns where primary call driver or reason for the customer outreach is underlined in the transcript. You can use this information to identify common emerging patterns across customer conversations.

Why don't I see color-coded bars on my Amazon Connect console?

If your Amazon Connect console 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 console.

You must have permissions to view unredacted content. For more information, see Security profile permissions for Contact Lens (p. 383).

About sentiment scores and non-talk time in Contact Lens

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 calls that are associated with varying degrees customer experiences, positive or negative. It helps them identify which of their calls to investigate.

To determine the sentiment score, Contact Lens for Amazon Connect analyzes the sentiment for every speaker turn during the conversation. It uses the frequency and proximity of the resulting sentiment for each speaker turn to assign a score that ranges from -5 to +5 for each portion of the call.

The final sentiment score for the entire conversation is an average of the scores assigned during the call.

Non-talk time

Contact Lens for Amazon Connect 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.

Non-talk time can be an indicator of calls that go poorly. For example, it may indicate that the customer was asking a question that's new for your contact center. Or it may indicate the agent didn't have a ready answer and needs more training.

About issue/call driver detection in Contact Lens

In the analyzed files that Contact Lens creates, and in the Amazon Connect console, you can identify potential customer issues (also known as call drivers) that need further investigation.

Contact Lens highlights the primary call driver or reason for the customer outreach in the call transcript. You can use this information to identify common emerging patterns across customer conversations.
Unlike the categorization of contacts, you don't need to configure issue detection to use this feature. Issues are detected based on an artificial intelligence analysis of each turn in the conversation.

Tip
Issues are highlighted only in conversations that occur after the release of the issue detection feature.

About loudness scores in Contact Lens

A loudness score measures how loudly someone is speaking. 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. Then you can investigate further by reading that portion of the transcript or listening to that section of the call.

For example, the following image shows where the customer is talking loudly and their sentiment is negative.

About sensitive data redaction in Contact Lens

To help you protect your customer's privacy, Contact Lens lets you automatically redact sensitive data from conversation transcripts and audio files. It redacts data, such as name and credit card information using Natural Language Understanding.

To enable redaction, choose the option on the Set recording and analytics behavior (p. 249) block. For more information, see How to enable redaction of sensitive data (p. 380).

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.

This feature is currently available in US English, AU English, GB English, and IN English.

**About redacted files**

Redacted files are stored in your Amazon S3 bucket: Connect-instanceARN / Analysis. You cannot access redacted files through the Amazon Connect console.

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](p. 400).
- 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** (p. 249) block. For an example file, see [Example original, analyzed file](p. 395).

**Important**
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). Sensitive data in audio files is redacted as silence. These silent times are not flagged in the Amazon Connect console or elsewhere as non-talk time.

Use your file retention policies to determine how long to keep these files.

**Example Contact Lens output files**

**Example output locations**

Following are examples of what Contact Lens output files look like 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
- 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
- Redacted audio file
  - /connect-instance- bucket/Analysis/Voice/Redacted/2020/02/04/contact's_ID_call_recording_redacted_2020-02-04T21:14:16Z.wav

**Example original, analyzed file**

This section shows an example schema for a conversation 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 Redacted section only if it includes PII.
- If a Redacted 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
{
    "Participants": [
        {
            "ParticipantId": "55555555-5555-5555-5555-55555555555",   //This is the agent's ARN. It's always long.
            "ParticipantRole": "AGENT"
        },
        {
            "ParticipantId": "33333333",  //This is the customer's ID. It's always short.
            "ParticipantRole": "CUSTOMER"
        }
    ],
    "Channel": "VOICE",
    "AccountId": "BBBBBBBBBBB",
    "Version": "1.1.0",
    "JobStatus": "COMPLETED",
    "LanguageCode": "en-US",
    "CustomModels": [{   //Large contact centers may want to use custom language models. If so, contact AWS support for help.
        "Type": "TRANSCRIPTION_VOCABULARY",
        "Name": "MostCommonKeywordsTranscriptionV1"
    },
    {
        "Type": "TEXT_ANALYSIS_ENTITIES",
        "Name": "Top100EntitiesV2"
    }],
    "ContentMetadata": {
        "Output": "Raw"  //Raw indicates this file includes sensitive data.
    },
    "CustomerMetadata": {
        "ContactId": "11111111-1111-1111-1111-11111111111",
        "InstanceId": "eeeeeee-eeee-eeee-eeee-eeeeeeeee"  
    },
    "Transcript": [
        {
            "ParticipantId": "55555555-5555-5555-5555-55555555555",
            "Id": "tttttttt-tttt-tttt-tttt-tttttttt",  //Each turn has an ID.
            "Content": "Hello, my name is Jane, may I have your email id?",
            "BeginOffsetMillis": 0,
            "EndOffsetMillis": 3000,
            "Sentiment": "NEUTRAL",  //The sentiment can be neutral, positive, negative, or mixed (some negative and positive, which is rare).
            "LoudnessScore": [   //This indicates the loudness score. Because it’s a three-second sentence, there are three loudness scores.
                40.5,              //The Amazon Connect console shows one bar for each of these values.
                55.0,
```
If a turn doesn't include sensitive data, there is no Redaction section.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.

If you delete this file, you won't see the email ID.
"Interruptions",
"MatchedDetails":{
  "Swearing":{
    "PointsOfInterest":[
      { "BeginOffsetMillis":0, //The swearing is called out with the beginning
                     and end offset.
      "EndOffsetMillis":300
    },
    { "BeginOffsetMillis":360,
      "EndOffsetMillis":500
    }
  }
  "Interruptions":{
    "PointsOfInterest":[
      { "BeginOffsetMillis":0, //The interruptions are called out with the
                     beginning and end offset.
      "EndOffsetMillis":500
    },
    { "BeginOffsetMillis":360,
      "EndOffsetMillis":500
    }
  }
}
"ConversationCharacteristics":{
  "TotalConversationDurationMillis":7060,
  "NonTalkTime":{
    "TotalTimeMillis":172,
    "Instances":[
      { "BeginOffsetMillis":3,
        "EndOffsetMillis":60,
        "DurationMillis":57
      },
      { "BeginOffsetMillis":45,
        "EndOffsetMillis":160,
        "DurationMillis":115
      }
    ]
  }
  "TalkTime":{
    "TotalTimeMillis":90000,
    "DetailsByParticipant":{
      "55555555-5555-5555-5555-55555555555":{
        "TotalTimeMillis":45000
      },
      "33333333":{
        "TotalTimeMillis":45000
      }
    }
  }
  "TalkSpeed":{
    "DetailsByParticipant":{
      "55555555-5555-5555-5555-55555555555":{
        "AverageWordsPerMinute":34
      },
      "33333333":{
        "AverageWordsPerMinute":40
      }
    }
  }
}

398
"Interruptions": {
   "TotalCount": 2,
   "TotalTimeMillis": 34,
   "InterruptionsByInterrupter": {
      "55555555-5555-5555-5555-55555555555": [
         { "BeginOffsetMillis": 3,
         "EndOffsetMillis": 34,
         "DurationMillis": 31 // This is how many milliseconds the agent talked over the customer. 
       },
         { "BeginOffsetMillis": 67,
         "EndOffsetMillis": 70,
         "DurationMillis": 3
       }
      ]
   },
   "Sentiment": {
      "OverallSentiment": {
         "55555555-5555-5555-5555-55555555555": 3, // The agent's overall sentiment score.
         "33333333": 4.2 // The customer's overall sentiment score.
      },
      "SentimentByPeriod": {
         "QUARTER": {
            "55555555-5555-5555-5555-55555555555": [
               { "BeginOffsetMillis": 0,
               "EndOffsetMillis": 100,
               "Score": 3.0
            },
               { "BeginOffsetMillis": 100,
               "EndOffsetMillis": 200,
               "Score": 3.1
            },
               { "BeginOffsetMillis": 200,
               "EndOffsetMillis": 300,
               "Score": 3.6
            },
               { "BeginOffsetMillis": 300,
               "EndOffsetMillis": 400,
               "Score": 3.1
            }
         }
      }
   }
}
Example redacted file

This section shows an example redacted file. It's a twin of the original analyzed file. The only difference is that sensitive data are redacted.

```json
{
    "Participants": [
        {
            "ParticipantId": "55555555-5555-5555-5555-55555555555",
            "ParticipantRole": "AGENT"
        },
        {
            "ParticipantId": "33333333",
            "ParticipantRole": "CUSTOMER"
        }
    ],
    "Channel": "VOICE",
    "AccountId": "BBBBBBBBBBB",
    "Version": "1.1.0",
    "JobStatus": "COMPLETED",
    "LanguageCode": "en-US",
    "CustomModels": [
        {
            "Type": "TRANSSCRIPTION_VOCABULARY",
            "Name": "MostCommonKeywordsTranscriptionV1"
        },
        {
            "Type": "TEXT_ANALYSIS_ENTITIES",
            "Name": "Top100EntitiesV2"
        }
    ],
    "ContentMetadata": {
        "RedactionTypes": ["PII"], // It says "PII" even though the redacted content could be other sensitive data such as credit card number.
        "Output": "Redacted"
    },
    "CustomerMetadata": {
        "ContactId": "11111111-1111-1111-1111-11111111111",
        "InstanceId": "eeeeeee-eeee-eeee-eeee-eeeeeeeeeeeee"
    },
    "Transcript": [
        {
            "ParticipantId": "55555555-5555-5555-5555-55555555555",
            "Id": "tttttttt-tttt-tttt-tttt-tttttttttttt",
            "Content": "Hello, my name is Jane, may I have your email id?",
```
"BeginOffsetMillis": 0,
"EndOffsetMillis": 300,
"Sentiment": "NEUTRAL",
"LoudnessScore": [40.5, 55.0, 59.3],
},

"ParticipantId": "33333333",
"Id": "ssssssss-ssss-ssss-ssss-ssssssssss",
"Content": "My email id is [PII].",
//This shows that the customer's email ID has been redacted.
"BeginOffsetMillis": 500,
"EndOffsetMillis": 945,
"Sentiment": "NEGATIVE",
"LoudnessScore": [40.5, 55.0, 59.3],
"Redaction": {
  "RedactedTimestamps": [
    {
      "BeginOffsetMillis": 900,
      "EndOffsetMillis": 944,
    }
  ],
},

"ParticipantId": "33333333",
"Id": "aaaaaaaa-aaaa-aaaa-aaaa-aaaaaaaaaaaa",
"Content": "Hi, I'm having trouble submitting the application, number [PII] 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": 1500,
"EndOffsetMillis": 1945,
"Sentiment": "NEGATIVE",
"LoudnessScore": [40.5, 55.0, 59.3],
"Redaction": {
  "RedactedTimestamps": [[
    "BeginOffsetMillis": 1610,
    "EndOffsetMillis": 1700
  ]],
},

"IssuesDetected": [{
  "CharacterOffsets": {
    "BeginOffsetChar": 0,
    "EndOffsetChar": 78
  },
  "Text": "Hi, I'm having trouble submitting the application, number [PII] on the portal. I tried but couldn't connect to my POC on the portal. So, I'm calling on this toll free number."
}]
},
"Categories": {
  "MatchedCategories": [
    "Greeting",
  "
"Interruptions",
"MatchedDetails" :{
  "Greeting" :{
    "PointsOfInterest" :[
      {
        "BeginOffsetMillis" :0,
        "EndOffsetMillis" :300
      },
      {
        "BeginOffsetMillis" :360,
        "EndOffsetMillis" :500
      }
    ]
  },
  "Interruptions" :{
    "PointsOfInterest" :[
      {
        "BeginOffsetMillis" :0,
        "EndOffsetMillis" :500
      },
      {
        "BeginOffsetMillis" :360,
        "EndOffsetMillis" :500
      }
    ]
  }
},
"ConversationCharacteristics" :{
  "TotalConversationDurationMillis" :7060,
  "NonTalkTime" :{
    "TotalTimeMillis" :172,
    "Instances" :[{
      "BeginOffsetMillis" :3,
      "EndOffsetMillis" :60,
      "DurationMillis" :57
    },
    {
      "BeginOffsetMillis" :45,
      "EndOffsetMillis" :160,
      "DurationMillis" :115
    }
  ]
},
"TalkTime" :{
  "TotalTimeMillis" :90000,
  "DetailsByParticipant" :{
    "55555555-5555-5555-5555-55555555555" :{
      "TotalTimeMillis" :45000
    },
    "33333333" :{
      "TotalTimeMillis" :45000
    }
  }
},
"TalkSpeed" :{
  "DetailsByParticipant" :{
    "55555555-5555-5555-5555-55555555555" :{
      "AverageWordsPerMinute" :34
    },
    "33333333" :{
      "AverageWordsPerMinute" :40
    }
  }
}
"Interruptions": {
  "TotalCount": 2,
  "TotalTimeMillis": 34,
  "InterruptionsByInterrupter": {
    "55555555-5555-5555-5555-55555555555": [
      { "BeginOffsetMillis": 3, "EndOffsetMillis": 34, "DurationMillis": 31 },
      { "BeginOffsetMillis": 67, "EndOffsetMillis": 70, "DurationMillis": 3 }
    ]
  }
},
"Sentiment": {
  "OverallSentiment": {
    "55555555-5555-5555-5555-55555555555": 3,
    "33333333": 4.2
  },
  "SentimentByPeriod": {
    "QUARTER": {
      "55555555-5555-5555-5555-55555555555": [
        { "BeginOffsetMillis": 0, "EndOffsetMillis": 100, "Score": 3.0 },
        { "BeginOffsetMillis": 100, "EndOffsetMillis": 200, "Score": 3.1 },
        { "BeginOffsetMillis": 200, "EndOffsetMillis": 300, "Score": 3.6 },
        { "BeginOffsetMillis": 300, "EndOffsetMillis": 400, "Score": 3.1 }
      ],
      "33333333": [
        { "BeginOffsetMillis": 0, "EndOffsetMillis": 100, "Score": 3.1 },
        { "BeginOffsetMillis": 100, "EndOffsetMillis": 200, "Score": 3.2 },
        { "BeginOffsetMillis": 200, "EndOffsetMillis": 300, "Score": 3.6 },
        { "BeginOffsetMillis": 300, "EndOffsetMillis": 400, "Score": 3.1 }
      ]
    }
  }
}
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 contact flow. When this happens, Contact Lens sends error notifications using Amazon EventBridge events.

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"

The following image shows what this looks like in EventBridge:

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:

```
{
    "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 contact 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 audio file is too small for analysis (less than 105 ms).</td>
</tr>
<tr>
<td>RECORDING_FILE_TOO_LARGE</td>
<td>The recording file exceeds the duration limit for analysis (more than 14,400 seconds, or 4 hours).</td>
</tr>
<tr>
<td>RECORDING_FILE_INVALID</td>
<td>The audio file is invalid.</td>
</tr>
<tr>
<td>RECORDING_FILE_CANT_READ</td>
<td>An error occurred when Contact Lens tried to read the audio file.</td>
</tr>
<tr>
<td>RECORDING_FILE_EMPTY</td>
<td>The audio file is empty.</td>
</tr>
<tr>
<td>RECORDING_SAMPLE_RATE_NOT_SUPPORTED</td>
<td>The sample rate of the audio file is not supported. Contact Lens currently supports audio files with an 8kHz sample rate. That is the sample rate for Amazon Connect recordings.</td>
</tr>
</tbody>
</table>
Monitor metrics and run reports

In Amazon Connect, data about contacts are captured in contact trace records (CTR). 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 CTR. When you create metrics reports, the values displayed for most (not all) metrics in the report are calculated using the data in the CTRs.

CTRs are available within your instance for 24 months from the time when the associated contact was initiated. You can also stream CTRs 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 (p. 474).

Contents
- What's new in metrics (p. 406)
- About agent status (p. 414)
- About contact states (p. 415)
- About queued callbacks in metrics (p. 417)
- Save custom reports (p. 422)
- Share custom reports (p. 424)
- View a shared report (p. 425)
- Publish reports (p. 426)
- Real-time metrics reports (p. 428)
- Historical metrics reports (p. 449)
- Search for contacts (p. 467)
- View a CTR in the UI (p. 469)
- Login/Logout reports (p. 470)
- Amazon Connect agent event streams (p. 474)
- Contact trace records (CTR) data model (p. 487)
- Monitoring your instance using CloudWatch (p. 497)
- Logging Amazon Connect API calls with AWS CloudTrail (p. 502)

What's new in metrics

Thanks to your feedback, we’ve made changes to Amazon Connect metrics. This topic gives you a overview of the improvements.

**Upcoming changes: Group by channel in a historical metrics report**

The following changes to the historical metrics report are upcoming in a future release.

**To group by channel on historical metrics reports**

1. On the navigation menu, choose Metrics and quality, 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**.

![Image of Table Settings](image1.png)

4. The table shows a column for **Channel**, as shown in the following image.

![Image of Historical metrics](image2.png)

**October 2020**

**New historical metrics for inbound and outbound contact time**

Released the following real-time metrics:

- Avg callback connecting time (p. 444)
- Avg incoming connecting time (p. 444)
- Avg outbound connecting time (p. 445)

Released the following historical metrics:

- Agent API connecting time (p. 457)
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.

For more information, see Use one-click drill-downs for Routing profiles and Queues tables (p. 430)

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 Metrics and quality, 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).

![Historical metrics: Agents](image)

### 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:

- $(\text{Agent on contact (wall clock time)} / (\text{Agent on contact (wall clock time)} + \text{Agent idle time}))$
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.

**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.
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>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>
</tbody>
</table>
### Scenario

<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 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>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>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>
</tbody>
</table>
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**
Supervisors can manually change the agent's status in the real-time metrics report (p. 438).

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 (p. 477).

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": { //Here's the agent's status that they set in the CCP.
      "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.
    }
  }
}
```

### 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.
Events in the contact trace record (CTR)

A contact trace record (CTR) 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 CTR, see Contact trace records (CTR) data model (p. 487).

A CTR is opened for a customer when they are connected to your contact center. The CTR is completed when the interaction with the contact flow or agent ends. This means it’s possible for a customer to have multiple CTRs.

The following diagram shows when a CTR is created for a contact.

- **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.

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.
    }
]
```
Each time a contact is connected to an agent, a new CTR is created. The CTRs for a contact are linked together through the contactId fields: original, next, and previous.

About queued callbacks in metrics

This topic explains how queued callbacks appear in your real-time metrics reports and the contact trace record (CTR).

**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 (p. 118). 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 (p. 270) block transfers the initial contact to a callback queue.

2. The callback is then placed in the queue. It remains there until an agent is available and can be offered the contact.

3. When the callback is connected to the agent, a new CTR is created for the contact.
4. The **Initiation Timestamp** in the callback CTR corresponds to when the Transfer to queue (p. 270) block transferred the contact to a callback queue, shown in step 1.

---

**How properties in the Transfer to Queue block affect this flow**

The Transfer to queue (p. 270) 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 contact 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 (p. 419).
• **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 (p. 270)** 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.

   ![Real-time metrics](image1)

2. After 35 seconds, the callback contact has been placed in queue.

   ![Real-time metrics](image2)

3. Assume that after 40 seconds, an agent accepts the callback.

   ![Real-time metrics](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 CTR:

The enqueued time on the CTR 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 CTRs.

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 CTRs:

1. The first CTR, with InitiationMethod=INBOUND, would have an enqueued time of 5 minutes.
2. The second CTR, 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 CTRs and times are set for it.
Assume we have set up the following contact flows:

- **Inbound contact 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 contact 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 contact flow creates CTR-1:
   a. John calls customer service at 11:35. The Inbound contact 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 contact flow creates CTR-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 CTRs, which include the following metadata.

<table>
<thead>
<tr>
<th>CTR-1</th>
<th>Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation Method</td>
<td>Inbound</td>
<td>The inbound contact is initiated in Amazon Connect.</td>
</tr>
<tr>
<td>Initiation Timestamp</td>
<td>11:35</td>
<td></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 CTR-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>
</tbody>
</table>
### CTR-1

<table>
<thead>
<tr>
<th>Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectedToAgent Timestamp</td>
<td>John scheduled a callback before any agent could pick up.</td>
</tr>
<tr>
<td>Disconnected Timestamp</td>
<td>John was disconnected by contact flow.</td>
</tr>
</tbody>
</table>

### CTR-2

<table>
<thead>
<tr>
<th>Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreviousContactId points to</td>
<td>The callback contact is created in Amazon Connect.</td>
</tr>
<tr>
<td>Initiation Timestamp</td>
<td>The contact was put into the CallbackQueue, after the 99-second initial delay completes.</td>
</tr>
<tr>
<td>Queue</td>
<td>After 21 seconds, an agent accepts the contact.</td>
</tr>
<tr>
<td>Enqueued Timestamp</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>Dequeued Timestamp</td>
<td>John is called after the 10 second agent whisper flow completes.</td>
</tr>
<tr>
<td>Queue Duration</td>
<td>John and the agent are connected, after the 15 second outbound whisper flow completes.</td>
</tr>
<tr>
<td>ConnectedToSystem Timestamp</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](p. 434) and [Create a historical metrics report](p. 450).

After you create a report, you can:

- **Save** (p. 423) the custom report and return to it later.
- **Share** (p. 424) a link to the custom report so only people in your organization who have the link AND who have the appropriate permissions (p. 425) in their security profile can access the report.
- **Publish** (p. 426) the report so everyone in your organization who has the appropriate permissions (p. 427) 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 (p. 566).

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, go to Metrics and quality, Saved reports.
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** and **Create saved reports**.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>Access</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access metrics</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>
</tr>
<tr>
<td>Contact attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login/Logout report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recorded conversations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saved reports</td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

This gives you access to real-time and historical metrics reports.

This gives you permission to create, share, and publish custom reports.

To share reports

1. On the report page, choose **Share report**.

Or, from your list of saved reports, choose the **Share report** icon.
2. Choose **Copy link address** and choose **Save**. 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
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 (p. 427) 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 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. Toggle Publish report to On, and then choose Save.
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**
To view published reports

- Go to Metrics and quality, Saved reports.

Published reports appear in your list automatically.

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 to create custom reports, such as real-time reports that are filtered by teams of agents.

Contents

- Permissions required to view real-time metrics reports (p. 429)
- How often real-time metrics refresh (p. 429)
- Use one-click drill-downs for Routing profiles and Queues tables (p. 430)
- View how many contacts are waiting in queue (p. 432)
- Create a real-time metrics report (p. 434)
- No metrics or too few rows in a queues report? (p. 435)
- List queues grouped by routing profile (p. 436)
- List agents grouped by routing profile (p. 436)
- Sort agents by activity in a real-time metrics report (p. 437)
- Change the "Agent activity" status in a real-time metrics report (p. 438)
• Download a real-time metrics report (p. 440)
• Real-time metrics definitions (p. 441)

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 **Access metrics** permission.

To create, share, and publish saved reports, you need the **Create** permission.

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>Access</th>
<th>View</th>
<th>Edit</th>
<th>Create</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access metrics</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>
</tr>
<tr>
<td>Contact attributes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login/Logout report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recorded conversations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saved reports</td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

This gives you access to real-time and historical metrics reports.

This gives you permission to create, share, and publish custom reports.

To view the agent's hierarchy information in a real-time metrics report, which can include their location and skill set data, you need the **View - Agent hierarchy** permission:

<table>
<thead>
<tr>
<th>Type</th>
<th>All</th>
<th>View</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent hierarchy</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Security profiles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent status</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</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 every 5 minutes.

• 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**.

Below the **Queues** table, a **Routing profiles** table appears. 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. The agents may be associated with different routing profiles.
View how many contacts are waiting in queue

To see the number of customers waiting in queue

1. Go to Metrics and quality, Real-time metrics, Queues.
2. By default, customers who are waiting for a call back are counted in the In queue column. This column counts all customers who are in a queue for an agent, not just the callback customers.

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 Metrics and quality, Real-time metrics, Queues.
2. Choose New table, Agent queues.
The **In queue** column displays how many contacts are in the agent's queue.

3. Review the metrics in then **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 the 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**.
2. Choose the **Metrics** tab.
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 (p. 361).

To create a real-time metrics report

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Metrics and Quality, Real-time metrics.
3. Choose one of the following report types, which 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.

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 (p. 441)**.

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 **Metrics and Quality, 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.

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 **Metrics and quality, 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 **Metrics and quality, Real-time metrics, Queues**.
2. Choose **New table, Agents**.
3. Click **Settings**.

4. On the **Filters** tab, choose **Routing profiles**. In **Include**, select the routing profiles you want included in the table.
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.

However, if one or more agents are enabled to handle both voice and chat contacts, you can't sort them by the **Activity** column because of the two channels. There's no option to sort by the **Activity** column, as shown in the following image:
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, supervisors can manually change the Agent Activity status of an agent. This overrides what the agent has set in the CCP.

When you choose the Agent Activity column, you can select a status, such as Offline, Available, or Break.

This change appears in the agent event stream.

You can't select or change any of the contact states that appear in the Agent Activity column, such as Incoming or On contact.
Change an agent's activity status

You'll get an error message, as shown in the following image.

Required permissions to change an agent's activity status

For someone such as a supervisor to be able to change an agent's activity status, they need to be assigned a security profile that has the following permissions:

- Edit/View Agent Status
- Access metrics
Download a real-time metrics report

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.
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.

### 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

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

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 is `SLOTS_ACTIVE`.

#### ACW

Count of contacts who are in an `AfterContactWork` state. After a conversation between an agent and customer ends, the contact is moved into the ACW state.
In the `GetCurrentMetricData` API, this metric is `AGENTS_AFTER_CONTACT_WORK`. The name of this metric is confusing because in the Amazon Connect console, ACW counts the number of contacts who are in an ACW state, not the number of agents.

To learn more about agent status and contact states, see About agent status (p. 414) and About contact states (p. 415).

**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 supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, then the supervisor’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**

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**

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**

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 (p. 126). 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 is `SLOTS AVAILABLE`.

**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 supervisor 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 is at maximum capacity. For example, they are only allowed to handle 3 contacts at a time and they are currently handling 3.
• 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 is AGENTS_AVAILABLE.

**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 (p. 414) and About contact states (p. 415).

**Avg callback connecting time**

Then average time between when callback contacts are initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

The following image shows the five parts that go into calculating Avg callback connecting time. It also shows what is in the agent event stream.

**Avg hold time**

Average time, in seconds, that a contact in the queue was on hold.

**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.

The following image shows the three parts that go into calculating Avg incoming connecting time. It also shows what is in the agent event stream.
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 contact 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.

The following image shows the four parts that go into calculating Avg outbound connecting time. It also shows what is in the agent event stream.

Callback contacts handled

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 (-).

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 supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, the superviser's contact state is Monitoring; the agent's contact state is Connected.

Duration
Amount of time that the agent has been in the current Agent Activity State.

Error
A count of agents in Error state.

In the GetCurrentMetricData API, this metric is AGENTS_ERROR.

Handled
Count of contacts in the queue that were answered by an agent.

Handled in
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
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
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

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 (p. 419).

In the GetCurrentMetricData API, this metric is 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)

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 is AGENTS_NON_PRODUCTIVE.

Occupancy

Percentage of time that an agent was active on contacts. This percentage is calculated as follows:

\[(\text{Agent on contact (wall clock time)} / (\text{Agent on contact (wall clock time)} + \text{Agent idle time}))\]

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 is OLDEST_CONTACT_AGE.

On contact

Count of agents currently on a contact. An agent is "on a contact" when they are handling at least one contact who is either connected, on hold, in After contact work, or outbound ring.

In the GetCurrentMetricData API, this metric is 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

Count of agents who have set their status in the CCP to something other than Offline. 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 (p. 443).

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 is AGENTS_ONLINE.

**Queue**

The name of the queue associated with the contact the agent is currently handling.

**Queued**

Count of contacts added to the queue during the specified time range.

**Routing Profile**

The routing profile for the agent.

**Scheduled**

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 (p. 419).

In the GetCurrentMetricData API, this metric is CONTACTS_SCHEDULED.

**SL X**

Percentage of contacts removed from the queue between 0 and X seconds 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. The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

**Staffed**

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 is `AGENTS_STAFFED`.

**Transferred in**

Count of contacts transferred into the queue during the specified time range.

**Transferred in from queue**

Count of contacts transferred into the queue from another queue during a **Customer queue flow**.

**Transferred out**

Count of contacts transferred out of the queue during the specified time range.

**Transferred out from queue**

Count of contacts transferred out of the queue to another queue during a **Customer queue flow**.

---

# 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:

**CTR-driven metrics**

These metrics are based on formed CTR records. For a given interval, CTRs 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 CTR-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

• Create a historical metrics report (p. 450)
• Historical report limits (p. 452)
• Schedule a historical metrics report (p. 453)
• Update a historical metrics report (p. 454)
• Download a historical metrics report (p. 454)
• Show agent queues in a Queues table (p. 456)
• About the agent activity audit report (p. 457)
• Historical metrics definitions (p. 457)

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 (p. 361).

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 your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose **Metrics and quality, 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**
     - **Agent metrics**
   - **Agents**
     - **Agent performance**
   - **Phone numbers**
   - **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 (p. 450).

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 (p. 451).

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 (p. 457).

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:

#### 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.

#### Download data limited to current page max (100 results)

- When you want to download historical metrics data into a .csv file from the user interface, you can only download the data displayed on the page at any one time. For example, if you have 256 records you want to download, and the maximum displayed in the user interface is 100, you would have to download the data three batches:
  - 1-100
  - 101-200
  - 201-256

   For a workaround so you can download hundreds or thousands of results, see Download all historical metric results (p. 455).

#### 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. Any user with permission to edit saved reports can also modify your scheduled reports.

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.

All scheduled reports use the UTC day, regardless of the timezone of the report

- For example, let's say you are in PST (Pacific Standard Time) and you schedule a Last 24 hours report to run at 16:00 every day. Here's the logic we use to run the report on May 15, 2020, for example:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time</td>
<td>2020-05-15T16:00:00.000Z</td>
</tr>
<tr>
<td>Minus 24 hours</td>
<td>2020-05-14T16:00:00.000Z</td>
</tr>
<tr>
<td>Get the date</td>
<td>2020-05-14</td>
</tr>
<tr>
<td>Get the time range</td>
<td>2020-05-14T00:00:00.000Z - 2020-05-15T00:00:00.000Z (this is the UTC day)</td>
</tr>
</tbody>
</table>
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 your contact center using your access URL (https://domain.awsapps.com/connect/login).
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.

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 your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Metrics and quality, 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.

Important
From the Amazon Connect console, you can only download the results currently displayed on the page. For example, if there are 256 results, but only 100 are displayed on the page at a time, you would need to download the data in three batches (1-100, 101-200, 201-256). For a workaround, see Download all historical metric results (p. 455).

To download a historical metrics report as a CSV file

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
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.

Although the times in the online report are in hh:mm:ss, all times in the downloaded report are in seconds.

![Excel sheet](image1.png)

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.

![Excel sheet](image2.png)

Tip: when you download a historical metrics report, the interval will be in ISO date 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 (p. 453).

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.

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.
3. Choose Apply. The agent queues you selected appear in the Queues table in the historical metrics report.

### About the agent activity audit report

The agent activity audit is like a report version of the agent event stream (p. 474). 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.

### What does Telecom issue mean?

If there's an error message on an agent activity audit report that says Telecom Issue, it means there was an error setting up the agent's connection to the voice service. For example, there was an error with their soft phone connection.

### Historical metrics definitions

The following metrics are available to include in historical metrics reports in Amazon Connect.

**Tip**
Developers can use the GetMetricData API to get a subset of the following historical metrics from the specified Amazon Connect instance.

#### After contact work time

The total time that an agent spent doing ACW for a contact.

You specify the amount of time an agent has to do ACW in their agent configuration settings (p. 131). 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.

- **Type:** String \( (hh:mm:ss) \)
- **Category:** CTR-driven metric

#### Agent answer rate

Percentage of contacts routed to an agent that were answered.

- **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.

- **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.

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.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric

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.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Agent interaction and hold time

Sum of Agent interaction time (p. 458) and Customer hold time (p. 466).

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

Agent interaction time

Total time that agents spent interacting with customers on inbound and outbound contacts. This does not include Customer Hold Time (p. 466) or After Contact Work Time (p. 457).

- Type: String (hh:mm:ss)
• Category: CTR-driven metric

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
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.

• Type: Integer
• Category: Agent activity-driven metric

Agent on contact time
Total time that an agent spent on a contact, including Customer Hold Time (p. 466) and After Contact Work Time (p. 457). This does not include time spent on a contact while in a custom status.

Tip
If you want to include the time spent in a custom status, see Contact handle time (p. 462).

• Type: String (hh:mm:ss)
• Category: Agent activity-driven metric

Agent outbound connecting time
The total time between when an outbound contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

Type: String (hh:mm:ss)
Category: Agent activity-driven metric

API contacts
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: CTR-driven metric

API contacts handled
Count of contacts that were initiated using an Amazon Connect API operation, such as StartOutboundVoiceContact, and handled by an agent.
• Type: Integer
• Category: CTR-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 (p. 488) (from the CTR) for all contacts included in the report, based on the selected filters.
• Type: String (hh:mm:ss)
• Category: CTR-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.
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.
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.
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 CTR: AgentInteractionDuration (p. 488) and CustomerHoldDuration (p. 488).
• Type: String (hh:mm:ss)
• Category: CTR-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 (p. 466) or After Contact Work Time (p. 457).

- Type: String (hh:mm:ss)
- Category: CTR-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.

- Type: String (hh:mm:ss)
- Category: Agent activity-driven metric

**Average customer hold time**

Average time that customers spent on hold while connected to an agent. This is calculated by averaging CustomerHoldDuration (p. 488) (from the CTR).

- Type: String (hh:mm:ss)
- Category: CTR-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.

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

**Average outbound after contact work time**

Average time that agents spent doing After Contact Work (ACW) for an outbound contact.

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

**Average outbound agent interaction time**

Average time that agents spent interacting with a customer during an outbound contact.

- Type: String (hh:mm:ss)
- Category: CTR-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 (p. 494) and DequeueTimestamp (p. 494) (from the CTR) 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.

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

Average queue answer time

Average time that contacts waited in the queue before being answered by an agent. This is the average of Duration (p. 494) (from the CTR).

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

Callback contacts

Count of contacts that were initiated from a queued callback.

- Type: Integer
- Category: CTR-driven metric

Callback contacts handled

Count of contacts that were initiated from a queued callback and handled by an agent.

- Type: Integer
- Category: CTR-driven metric

Contact flow time

Total time a contact spent in a contact flow.

Outbound contacts don't start in a contact flow, so outbound contacts aren't included.

- Type: String (hh:mm:ss)
- Category: CTR-driven metric

Contact handle time

Total time that an agent spent on contacts, including Customer Hold Time (p. 466) and After contact work time (p. 457). This includes any time spent on contacts while in a custom status.

Tip
If you want to exclude the amount of time spent in a custom status, see Agent on contact time (p. 459).

- Type: String (hh:mm:ss)
• Category: CTR-driven metric

**Contact abandoned**

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**.

• Type: Integer
• Category: CTR-driven metric

**Contacts abandoned in X seconds**

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.

• Type: Integer
• Category: CTR-driven metric

**Contacts agent hung up first**

Count of contacts disconnected where the agent disconnected before the customer.

• Type: Integer
• Category: CTR-driven metric

**Contacts answered in X seconds**

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** (p. 494). The possible values for $X$ are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

• Type: Integer
• Category: CTR-driven metric

**Contacts consulted**

Deprecated May 2019. When used in a report, it returns a dash (-).

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.

• Type: Integer
• Category: CTR-driven metric

**Contacts handled**

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**.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts handled incoming

Count of incoming contacts that were handled by an agent, including inbound contacts and transferred contacts.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts handled outbound

Count of outbound contacts that were handled by an agent. This includes contacts that were initiated by an agent using the CCP.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts hold agent disconnect

Count of contacts that were disconnected by the agent while the customer was on hold.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts hold customer disconnect

Count of contacts that were disconnected by the customer while the customer was on hold.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts hold disconnect

Count of contacts disconnected while the customer was on hold. This includes both contacts disconnected by the agent and contacts disconnected by the customer.

- **Type:** Integer
- **Category:** CTR-driven metric

### Contacts incoming

Count of incoming contacts, including inbound contacts and transferred contacts.

- **Type:** Integer
- **Category:** CTR-driven metric
Contacts missed

Count of contacts routed to an agent but not answered by the agent, including contacts abandoned by the customer. A contact can be counted as missed multiple times, once for each time it is routed to an agent but not answered.

When you add this to a historical metrics report, it appears under the column named Agent non-response.

- Type: Integer
- Category: Agent activity-driven metric

Contacts put on hold

Count of contacts put on hold by an agent one or more times.

- Type: Integer
- Category: CTR-driven metric

Contacts queued

Count of contacts placed in the queue.

- Type: Integer
- Category: CTR-driven metric

Contacts transferred in

Count of contacts transferred to the queue by an agent using the CCP.

- Type: Integer
- Category: CTR-driven metric

Contacts transferred in from queue

Count of contacts transferred to the queue from another in a Transfer to queue contact flow.

- Type: Integer
- Category: CTR-driven metric

Contacts transferred out

Count of contacts transferred from the queue after being answered by an agent.

- Type: Integer
- Category: CTR-driven metric

Contacts transferred out external

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.
• Type: Integer
• Category: CTR-driven metric

Contacts transferred out queue

Count of contacts transferred from the queue to another queue in a Transfer to queue contact flow.

• Type: Integer
• Category: CTR-driven metric

Contacts transferred out internal

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.

• Type: Integer
• Category: CTR-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.

• Type: String (hh:mm:ss)
• Category: CTR-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.

• 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.

• Type: String (hh:mm:ss)
• Category: CTR-driven metric

Non-Productive Time

Total time that agents spent in a custom status (p. 130). 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.

This metric can't be grouped or filtered by queue.

- **Type:** String \((hh:mm:ss)\)
- **Category:** Agent activity-driven metric

## Occupancy

Percentage of time that agents were active on contacts. This percentage is calculated as follows:

\[
\text{Occupancy} = \frac{\text{Agent on contact (wall clock time)}}{\text{Agent on contact (wall clock time)} + \text{Agent idle time}}
\]

**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.

- **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. This metric can't be grouped or filtered by queue.

- **Type:** String
- **Category:** Agent activity-driven metric

## Service level X seconds

Percentage of contacts removed from the queue between 0 and \(X\) seconds 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. The possible values for \(X\) are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600. This percentage is calculated as follows:

\[
\left(\frac{\text{Contacts removed from queue in } X \text{ seconds}}{\text{Contacts queued}}\right) \times 100
\]

- **Type:** String
- **Min value:** 0.00%
- **Max value:** 100.00%
- **Category:** CTR-driven metric

## Search for contacts

You can search for contacts as far back as two years ago, 14 days at a time.

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.

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 \texttt{CallCenterManager} security profile, or to have the following permissions:

\begin{itemize}
  \item \textbf{Access metrics - Access}: Grants access to metrics data.
  \item \textbf{Contact search - View}: Grants access to the Contact search page, and the ability to search for contacts.
  \item \textbf{Restrict contact access}: Manage a user's access to results on the Contact search page based on their agent hierarchy group.
\end{itemize}

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 \textit{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, \texttt{All = View} since \texttt{View} is the only action granted.

For more information about hierarchy groups, see \textit{Set up agent hierarchies (p. 129)}.

\textbf{Note}

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.
• **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 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.

By default, the Amazon Connect **Admin** and **CallCenterManager** security profiles have these permissions.

For information about how add more permissions to an existing security profile, see **Update security profiles** (p. 366).

### How to search for a contact

1. Log in to Amazon Connect with a user account that has **permissions to access contact records** (p. 468).
2. In Amazon Connect choose **Metrics and quality**, **Contact search**.
3. Use the filters on the page to narrow your search. For date, you can search up to 14 days at a time.
4. To see additional columns in your search results, expand **Additional fields** to choose what other data you want to view. Choose **Apply** to view the columns.

   **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.

### View a CTR in the UI

1. Do a **contact search** (p. 467). A list of contact IDs will be returned.
2. Choose an ID to view the CTR for the contact.

The following image shows part of a CTR 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.
Login/Logout reports

The Login/Logout report displays the login and logout information for the agents in your contact center. For each agent session, the login and logout times are displayed as a row in the report. You can use the report to determine the time your agents were logged in to Amazon Connect. The report also displays the amount of time for each session that an agent 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 (p. 133), agents must choose the **Logout** button. Until they choose the **Logout** button, the Login/Logout report shows them as logged in.

**Login/Logout report limit: 10,000 rows**

- If you try to generate a Login/Logout report that has more than 10,000 rows, it won’t complete.
- The Login/Logout report page displays only 10,000.
• If you schedule a Login/Logout 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 agents, 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/Logout report

Before you can generate a Login/Logout report, you need the following permissions assigned to your security profile: Login/Logout report - View.

By default, the Amazon Connect Admin security profile has these permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 366).

Generate a Login/Logout report

A Login/Logout report includes only login or logout actions by your agents that occurred during the specified time range.

• If an agent logged in during the time range and did not log out, the report shows a login time but not a logout time.
• If the agent 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 agent session associated with the most recent logout.

To generate a Login/Logout report

1. Open your Amazon Connect dashboard.
2. Choose **Metrics and Quality, 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.

![Login/Logout report](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. Open your Amazon Connect dashboard.
2. Choose **Metrics and quality, 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. 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.

When you schedule your report, keep in mind that the report always runs at 12AM on the day you select, in the time zone that you choose. 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.

Tip
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.

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 Metrics and quality, 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: ...

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 Metrics and quality, Saved reports.
3. Hover over the row for the report to delete, and choose the Delete icon.
4. Choose Delete again.

**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 (p. 475)
- Sample agent event stream (p. 475)
- Determine how long an agent spends doing ACW (p. 477)
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 trace 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 a customer master key (CMK) using KMS for encryption. Finally, choose the same CMK 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 customer master key (CMK) 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 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.

```json
{
"AWSAccountId": "012345678901",
"CurrentAgentSnapshot": {
  "AgentStatus": {
    "Name": "Offline",  // The agent is offline.
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
  },
  "Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "AgentEventStreamTest",
    "LastName": "Agent",
    "RoutingProfile": {
    }
}
```
"Concurrency": [
    {
      "AvailableSlots": 3,  // This shows the agent has 3 slots available. They aren't on any chats right now.
      "Channel": "CHAT",
      "MaximumSlots": 3  // The agent's routing profile allows them to take up to 3 chats.
    },
    {
      "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": {
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.

```json
{
    "AWSAccountId": "012345678901",
    "CurrentAgentSnapshot": {
        "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": [
                {
                    "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).
            "InitialContactId": null,
            "Name": "ContactName-1"
        }
    ]
}
```
"InitiationMethod": "OUTBOUND", //This indicates how the contact was initiated. OUTBOUND means the agent initiated contact with the customer.
    INBOUND means the customer initiated contact with your center.
"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": [ {
                "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", //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".
}
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": [  
   {  
   "Name": "BasicQueue"  
   }  
   ]  
   }  
   }  
   }  
   }  
   }
   ```
Determine how long an agent spends doing ACW

```
{
    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
    "Name": "PrimaryQueue"
}
}

//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.
    },
    "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 ContactId of the customer the agent was working on previously.
            "InitialContactId": null,
            "InitiationMethod": "OUTBOUND",
```
"Queue": {
  "Name": "BasicQueue"
},
"QueueTimestamp": null,
"State": "ENDED", //The ACW for ContactId-1 has ended.
}
]
"Version": "2019-05-25"
}

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
    - Phone type: soft phone or desk phone
    - 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.

Event Objects

- AgentEvent (p. 483)
- AgentSnapshot (p. 484)
- Configuration (p. 484)
- Contact object (p. 485)
- HierarchyGroup object (p. 486)
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: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. Not applicable to LOGIN or LOGOUT events.

Type: AgentSnapshot object

**Version**

The version of the agent event stream in date format, such as 2019-05-25.
AgentSnapshot

The AgentSnapshot object includes the following properties:

AgentStatus

Agent status data, including:
- AgentARN—The ARN for the agent.
- Name—This is the status of the agent that they manually set in the CCP (p. 414), or that the supervisor manually changes in the real-time metrics report (p. 438).

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:ssZ)

Type: AgentStatus 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: ContactList object

Configuration

The Configuration object includes the following properties:

FirstName

The first name entered in the agent's Amazon Connect account.

Type: String

Length: 1-100

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*

**InitiationMethod**

Indicates how the contact was initiated.

*Valid values: INBOUND | OUTBOUND | TRANSFER | CALLBACK | QUEUE_TRANSFER | API*

**State**

The state of the contact.

*Valid values: INCOMING | PENDING | CONNECTING | CONNECTED | CONNECTED_ONHOLD | MISSED | ERROR | ENDED*

**StateStartTimestamp**

The time at which the contact entered the current state.
Type: String (yyyy-mm-ddThh:mm:ssZ)

**ConnectedToAgentTimestamp**

The time at which the contact was connected to an agent.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**QueueTimestamp**

The time at which the contact was put into a queue.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**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.

Type: `HierarchyGroup` object

**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

**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

**Contact trace records (CTR) data model**

This article describes the data model for Amazon Connect contact trace records (CTRs). CTRs capture the events associated with a contact in your contact center. Real-time and historical metrics are based on the data captured in the CTRs.

For the CTR retention period and maximum size of the CTR attributes section, see the Feature specifications (p. 568).
Tip
Amazon Connect delivers CTRs at least once. CTRs may be delivered again for multiple reasons, such as new information arriving after initial delivery. If you're building a system that consumes CTR export streams, be sure to include logic that checks for duplicate CTRs 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.

Agent
Information about the agent who accepted the incoming contact.

AgentInteractionDuration
The time, in whole seconds, that an agent interacted with a customer.
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

HierarchyGroups
The agent hierarchy groups for the agent.
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 (p. 489)
Level2
The group at level two of the agent hierarchy.
Type: AgentHierarchyGroup (p. 489)

Level3
The group at level three of the agent hierarchy.
Type: AgentHierarchyGroup (p. 489)

Level4
The group at level four of the agent hierarchy.
Type: AgentHierarchyGroup (p. 489)

Level5
The group at level five of the agent hierarchy.
Type: AgentHierarchyGroup (p. 489)

ContactDetails
Contains user-defined attributes which are lightly typed within the contact.

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 (p. 488)
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

AWSContactTraceRecordFormatVersion

The record format version.

Type: String

Channel

How the customer reached your contact center.

Valid values: Voice, Chat

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 endpoint.

Type: Endpoint (p. 493)

DisconnectTimestamp

The date and time that the customer endpoint disconnected from Amazon Connect, in UTC time.

Type: String (yyyy-mm-ddThh:mm:ssZ)

InitialContactId

If this contact is related to other contacts, this is the ID of the initial contact.

Type: String
Length: 1-256

**InitiationMethod**

Indicates how the contact was initiated.

Valid values:
- **INBOUND**: The customer initiates voice (phone) contact with your contact center.
- **OUTBOUND**: An agent initiates voice (phone) contact with the customer, by using the CCP to call their number. This initiation method calls the `StartOutboundVoiceContact` API.
- **TRANSFER**: The customer is 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 is contacted as part of a callback flow.
- **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 is in one queue (listening to Customer queue flow), they are transferred into another queue using a contact flow block.
- **DISCONNECT**: When a `Set disconnect flow` block is triggered, a new contact is created. The block specifies which contact flow to run after a disconnect event during a conversation. A disconnect event is when an agent disconnects. When the disconnect event occurs, the corresponding content flow runs.

**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 **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` (p. 494)

**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 (p. 494)

Recording

If recording was enabled, this is information about the recording.

Type: RecordingInfo (p. 494)

Recordings

If recording was enabled, this is information about the recording.

Type: RecordingsInfo (p. 495)

Note

The first recording for a contact will appear in both the Recording and Recordings sections of the CTR.

SystemEndpoint

The system endpoint. For INBOUND, this is the phone number that the customer dialed. For OUTBOUND, this is the caller ID phone number that Amazon Connect used to dial the customer.

Type: Endpoint (p. 493)

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 (p. 493)

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

MediaStream

Information about the media stream used during the contact.

Type

Type: MediaStreamType

Valid value: AUDIO, VIDEO, CHAT

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 contact was connected to an agent.

Type: String (yyyyMMdd-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 (yyyyMMdd-ddThh:mm:ssZ)

Name

The name of the queue.

Type: String

Length: 1-256

RecordingInfo

Information about a voice recording.
RecordingsInfo

Information about a voice recording or chat transcript.

**DeletionReason**

If the recording/transcript 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 or chat transcript.

**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.

Type: String

**StartTime**

When the conversation started.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**Status**

The status of the recording/transcript.

Valid values: AVAILABLE | DELETED | NULL

**StopTime**

When the conversation stopped.

Type: String (yyyy-mm-ddThh:mm:ssZ)

**StorageType**

Where the recording/transcript is stored.

Type: String

Valid values: Amazon S3

**References**

Contains links to other documents that are related to a contact.

**Reference Info**

- ReferenceType
- ContentType
- Location

**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
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 CTR 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.

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.

Amazon Connect metrics sent to CloudWatch

The AWS/Connect namespace includes the following metrics.

**CallsBreachingConcurrencyQuota**

The total number of voice calls that exceeded the concurrent calls quota for the instance.

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
- **MetricGroup**: VoiceCalls

**CallBackNotDialableNumber**

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.
Amazon Connect Administrator Guide
Amazon Connect metrics sent to CloudWatch

Unit: Count

Dimensions:
• InstanceId: The ID of your instance
• MetricGroup: ContactFlow
• ContactFlowName: The name of your contact flow

CallRecordingUploadError

The number of call recordings that failed to upload to the Amazon S3 bucket configured for your instance. This is the bucket specified in Data Storage > Call Recordings settings for the instance.

Unit: Count

Dimensions:
• InstanceId: The ID of your instance
• MetricGroup: CallRecordings

CallsPerInterval

The number of voice calls, both inbound and outbound, received or placed per second in the instance.

Unit: Count

Dimensions:
• InstanceId: The ID of your instance
• MetricGroup: VoiceCalls

ConcurrentCalls

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.

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.

Unit: Count

Dimensions:
• InstanceId: The ID of your instance
• MetricGroup: VoiceCalls

ConcurrentCallsPercentage

The percentage of the concurrent active voice calls service quota used in the instance. This is calculated by ConcurrentCalls/ConfiguredConcurrentCallsLimit.

Unit: Percent (output displays as a decimal)

Dimensions:
• InstanceId: The ID of your instance
• MetricGroup: VoiceCalls

ContactFlowErrors

The number of times the error branch for a contact flow was executed.
Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: ContactFlow
- **ContactFlowName**: The name of your contact flow

**ContactFlowFatalErrors**
The number of times a contact flow failed to execute due to a system error.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: ContactFlow
- **ContactFlowName**: The name of your contact flow

**LongestQueueWaitTime**
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.

Unit: Seconds

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: Queue
- **QueueName**: The name of your queue

**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: Seconds

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: VoiceCalls

**MisconfiguredPhoneNumbers**
The number of calls that failed because the phone number is not associated with a contact flow.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: VoiceCalls

**PublicSigningKeyUsage**
The number of times a contact flow security key (public signing key) was used to encrypt customer input in a contact flow.
QueueCapacityExceededError

The number of calls that were rejected because the queue was full.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **SigningKeyId**: The ID of your signing key

QueueSize

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.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: Queue
- **QueueName**: The name of your queue

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

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 1, 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. The following dimensions are used in the CloudWatch dashboard for Amazon Connect 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. The following dimensions are used for Amazon Connect metrics in CloudWatch.

**Contact flow metrics dimension**

**Note**
If a contact flow has a dimension name in non-ASCII characters, you won't be able to see it in CloudWatch.

Filters metric data by contact flow. Includes the following metrics:

• ContactFlowErrors
• ContactFlowFatalErrors
• PublicSigningKeyUsage

**Instance metrics dimension**

Filters metadata by instance. Includes the following metrics:

• CallsBreachingConcurrencyQuota
• CallsPerInterval
• CallRecordingUploadError
• ConcurrentCalls
• ConcurrentCallsPercentage
• MisconfiguredPhoneNumbers
• MissedCalls
• 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:
Use CloudWatch metrics to calculate concurrent call quota

Here's how to calculate your quota for concurrent calls.

With calls active in the system, look at **ConcurrentCalls** and **ConcurrentCallsPercentage**. Calculate the quota:

\[
\text{quota} = \left( \frac{\text{ConcurrentCalls}}{\text{ConcurrentCallsPercentage}} \right) \times 100
\]

For example, if **ConcurrentCalls** is 20 and **ConcurrentCallsPercentage** is 50, your quota is calculated as

\[
\left( \frac{20}{50} \right) \times 100 = 40.
\]

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.

**Note**

Events from the Amazon Connect admin console aren't recorded in CloudTrail.

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 and Receiving CloudTrail Log Files from Multiple Accounts

Amazon Connect supports logging both the request parameters and the responses for the following APIs as events in CloudTrail log files:

• **Amazon Connect Service APIs**
  • AssociateRoutingProfileQueues
  • CreateContactFlow
  • CreateRoutingProfile
  • CreateUser
  • DeleteRoutingProfile
  • DeleteUser
  • DisassociateRoutingProfileQueues
  • StartChatContact
  • StartOutboundVoiceContact
  • StopContact
  • TagResource
  • UntagResource
  • UpdateContactFlowContent
  • UpdateContactFlowName
  • UpdateContactAttributes
  • UpdateRoutingProfileConcurrency
  • UpdateRoutingProfileName
  • UpdateRoutingProfileQueues
  • UpdateUserHierarchys
  • UpdateUserIdentityInfo
  • UpdateUserPhoneConfig
  • UpdateUserRoutingProfile
  • UpdateUserSecurityProfiles

• **Amazon Connect Participant Service APIs**
  • CreateParticipantConnection
  • DisconnectParticipant
  • SendEvent
  • SendMessage

For the following APIs, the request parameters are logged, but the responses are redacted:

• **Amazon Connect Service APIs**
  • DescribeContactFlow
  • DescribeRoutingProfile
  • DescribeUser
  • DescribeUserHierarchys
  • DescribeUserHierarchyGroup
  • DescribeUserHierarchyStructure
Example: Amazon Connect log file entries

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) user 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": "AAAAAAA1111111EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/John",
        "accountId": "123456789012",
        "accessKeyId": "AAAAAAA1111111EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-08-15T06:40:14Z"
            }
        }
    }
}
```
"sessionIssuer": {
    "type": "Role",
    "principalId": "AAAAAA111111EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/John",
    "accountId": "123456789012",
    "userName": "John"
}

"eventTime": "2019-08-15T06:40:55Z",
"eventSource": "connect.amazonaws.com",
"eventName": "GetContactAttributes",
"awsRegion": "us-west-2",
"sourceIPAddress": "205.251.233.179",
"userAgent": "aws-sdk-java/1.11.590 Mac_OS_X/10.14.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.202-b08 java/1.8.0_202 vendor/Oracle_Corporation",
"requestParameters": {
    "InitialContactId": "00fbeee1-123e-111e-93e3-11111bfbecc1",
    "InstanceId": "00fbeee1-123e-111e-93e3-11111bfbecc1"
},
"responseElements": null,
"requestID": "be1bee1d-1111-11e1-1eD1-0dc1111f111c",
"eventID": "00fbeee1-123e-111e-93e3-11111bfbecc1",
"readOnly": true,
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
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 (p. 506)
- Identity and access management for Amazon Connect (p. 509)
- Logging and monitoring Amazon Connect (p. 532)
- Compliance validation in Amazon Connect (p. 533)
- Resilience in Amazon Connect (p. 534)
- Infrastructure security in Amazon Connect (p. 535)

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. This content includes 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 user accounts with 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 recommend TLS 1.2 or later.
- 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 personal 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 sensitive identifying information, such as your customers' account numbers, into free-form 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 Amazon Connect or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

Contents
- Data handled by Amazon Connect (p. 507)
- Encryption at rest (p. 509)
- Encryption in transit (p. 509)
- Key management (p. 509)

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, contact flows, users, and routing profiles.
- **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.

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.

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 contact 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**

Call recording is disabled by default in Amazon Connect. You can enable call recording in the contact flows, which allows for more detailed control over which calls are recorded.

The call recording feature has options for choosing whether to record the agent only, customer only, or agent and customer conversations. When call recording is enabled, the recording begins when the call is connected to an agent and stops when the agent disconnects. Any transfers to external numbers are not recorded after the agent leaves the call.

You can limit access to the call recordings based on user permissions. Recordings can be searched and played back within the Amazon Connect web interface.

**Call recording storage**

Call recordings are stored in two phases:

- Recordings intermediately held within Amazon Connect during and after the call, but before delivery.
- Recordings delivered to your Amazon S3 bucket.

The recordings that are stored in your Amazon S3 bucket are secured using an AWS 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.

**Call recording access**

You can search and listen to call recordings in Amazon Connect. To determine which users can do this, assign them the appropriate security profiles. 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.

In addition, you can track who listens to or deletes recordings; see Track who deleted or listened to recordings (p. 373).

**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 ANI or other attributes set by the contact flow, that are associated with a contact for diagnostics or reporting purposes.

Contact data classified as PII, or data that represents customer content being stored by Amazon Connect, is encrypted at rest using a key that is time-limited and specific to the Amazon Connect instance.

The following data stored by Amazon Connect is treated as sensitive:

- Customer ANI
- Outbound phone number
- External numbers dialed by agents for transfers
Encryption at rest

Contact data classified as PII, or data that represents customer content being stored by Amazon Connect, is encrypted at rest using a key that is time-limited and specific to the Amazon Connect instance.

Amazon S3 server-side encryption is used to encrypt call recordings at rest using a customer-owned KMS key.

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? (p. 535)

When Amazon Connect integrates with AWS services, such as AWS Lambda, Amazon Kinesis, or Amazon Polly, data 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.

For information about AWS KMS keys see What is AWS Key Management Service? in the AWS Key Management Service Developer Guide.

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 (p. 509)
- Authenticating with identities (p. 510)
- Managing access using policies (p. 512)
- Required permissions for managing access to the Amazon Connect console (p. 513)
- How Amazon Connect works with IAM (p. 521)
- Amazon Connect identity-based policy examples (p. 524)
- Amazon Connect resource-level policy examples (p. 527)
- Troubleshooting Amazon Connect identity and access (p. 529)
- Use Service-Linked Roles for Amazon Connect (p. 531)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work 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 (p. 529).

### 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 employees 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 (p. 521).

### 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 (p. 524).

### Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see The IAM Console and Sign-in Page in the IAM User Guide.

You must be authenticated (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication, or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email or your IAM user name. You can access AWS programatically using your root user or IAM user access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don’t use AWS tools, you must sign the request yourself. Do this using Signature Version 4, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the AWS General Reference.

Regardless of the authentication method that you use, you might also 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 Using Multi-Factor Authentication (MFA) in AWS in the IAM User Guide.

### AWS account root user

When you first create an AWS account, you begin with a single 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 do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

### IAM users and groups

An IAM user is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing Access Keys for IAM Users in the IAM User Guide. When you generate access keys for an IAM user, make sure you view and securely save the key
pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

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:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.

- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the IAM User Guide.

- **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.

- **AWS service access** – A service role is an IAM role that a service assumes to perform actions in your account on your behalf. When you set up some AWS service environments, you must define a role for the service to assume. This service role must include all the permissions that are required for the service to access the AWS resources that it needs. Service roles vary from service to service, but many allow you to choose your permissions as long as you meet the documented requirements for that service. Service roles provide access only within your account and cannot be used to grant access to services in other accounts. You can create, modify, and delete a service role from within IAM. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the IAM User Guide.

- **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, 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an entity (root user, IAM user, or IAM role) 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.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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, role, or group. These policies control what actions that identity 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 such as an Amazon S3 bucket. Service administrators can use these policies to define what actions a specified principal (account member, user, or role) can perform on that resource and under what conditions. Resource-based policies are inline policies. There are no managed resource-based policies.

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 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 managing access to the Amazon Connect console

To allow read-only access, you need to attach only the AmazonConnectReadOnlyAccess policy.

To manage your Amazon Connect instance using 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:* grants your users all of the Amazon Connect permissions listed in this article.

### Amazon Connect console home page

The following image shows a sample Amazon Connect console home page.

![Amazon Connect virtual contact center instances](image)

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/ current settings</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:GetDataStreamConfig</td>
</tr>
<tr>
<td></td>
<td>connect:GetMediaStreamingConfig</td>
</tr>
<tr>
<td></td>
<td>connect:ListLambdaFunctions</td>
</tr>
<tr>
<td></td>
<td>connect:ListLexBots</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------</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>
<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>iam:AttachRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</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>
<tr>
<td></td>
<td>servicequotas:GetServiceQuota</td>
</tr>
</tbody>
</table>
**Required permissions for custom IAM policies**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
| Delete instance | connect:DestroyInstance  
|                 | connect:DescribeInstance  
|                 | connect:DeleteInstance  
|                 | connect:ListInstances  
|                 | ds:DescribeDirectories  
|                 | ds:DeleteDirectory  
|                 | ds:UnauthorizeApplication |

**Detailed instance pages**

The following image shows how you navigate to each of the detailed instance pages:

![Detailed instance pages](image)

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 and Telephony options pages

<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:ModifyInstance</td>
</tr>
<tr>
<td></td>
<td>connect:UpdateInstanceAttribute</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>
</tbody>
</table>
### Required permissions for custom IAM policies

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
|                                 | connect:ListInstanceStorageConfigs  
|                                 | connect:DescribeInstanceStorageConfig                                                |
| Edit call recording             | connect:ModifyInstance  
|                                 | connect:AssociateInstanceStorageConfig                                              |
|                                 | connect:UpdateInstanceStorageConfig                                                |
|                                 | connect:DisassociateInstanceStorageConfig                                           |
|                                 | s3:ListAllMyBuckets                                                                |
|                                 | s3:GetBucketLocation                                                               |
|                                 | s3:GetBucketAcl                                                                    |
|                                 | s3:CreateBucket                                                                    |
|                                 | kms:CreateGrant                                                                    |
|                                 | kms:DescribeKey                                                                    |
|                                 | kms:ListAliases                                                                    |
|                                 | kms:RetireGrant                                                                    |
|                                 | iam:PutRolePolicy                                                                  |
|                                 | iam:AttachRolePolicy                                                               |

### Chat transcripts section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
| View chat transcripts           | connect:DescribeInstance  
|                                 | connect:DescribeInstanceStorageConfig                                              |
|                                 | connect:ListInstanceStorageConfigs                                                |
| Edit chat transcripts           | connect:DescribeInstance  
|                                 | connect:AssociateInstanceStorageConfig                                              |
|                                 | connect:DisassociateInstanceStorageConfig                                           |
|                                 | connect:AssociateInstanceStorageConfig                                              |
|                                 | connect:UpdateInstanceStorageConfig                                                |
|                                 | connect:DisassociateInstanceStorageConfig                                           |
|                                 | s3:ListAllMyBuckets                                                                |
|                                 | s3:GetBucketLocation                                                               |

516
### Required permissions for custom IAM policies

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</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:GetMediaStreamingConfig</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:UpdateMediaStreamingConfig</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>kms:CreateGrant</td>
</tr>
<tr>
<td></td>
<td>kms:DescribeKey</td>
</tr>
<tr>
<td></td>
<td>kms:RetireGrant</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</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></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit exported reports</td>
<td>connect:ModifyInstance</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>connect:AssociateInstanceStorageConfig</td>
<td></td>
</tr>
<tr>
<td>connect:UpdateInstanceStorageConfig</td>
<td></td>
</tr>
<tr>
<td>connect:DisassociateInstanceStorageConfig</td>
<td></td>
</tr>
<tr>
<td>s3:ListAllMyBuckets</td>
<td></td>
</tr>
<tr>
<td>s3:GetBucketLocation</td>
<td></td>
</tr>
<tr>
<td>s3:CreateBucket</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>
<tr>
<td>kms:CreateGrant</td>
<td></td>
</tr>
<tr>
<td>iam:PutRolePolicy</td>
<td></td>
</tr>
<tr>
<td>iam:AttachRolePolicy</td>
<td></td>
</tr>
</tbody>
</table>

### Data streaming page

**Contact trace records section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
</table>
| View data streaming - Contact trace records | connect:GetDataStreamConfig  
connect:DescribeInstance  
connect:ListInstanceStorageConfigs  
connect:DescribeInstanceStorageConfig |
| Edit contact trace record | connect:UpdateDataStreamConfig  
connect:ModifyInstance  
connect:AssociateInstanceStorageConfig  
connect:UpdateInstanceStorageConfig  
connect:DisassociateInstanceStorageConfig  
connect:DescribeInstance  
firehose:ListDeliveryStreams  
firehose:DescribeDeliveryStream  
kinesis:ListStreams  
kinesis:DescribeStream |
### Required permissions for custom IAM policies

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</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:GetDataStreamConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListInstanceStorageConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceStorageConfig</td>
</tr>
<tr>
<td>Edit agent events</td>
<td>connect:UpdateDataStreamConfig</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstance</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>kinesis:ListStreams</td>
</tr>
<tr>
<td></td>
<td>kinesis: DescribeStream</td>
</tr>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</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:ModifyInstance</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateApprovedOrigin</td>
</tr>
<tr>
<td></td>
<td>connect:ListApprovedOrigins</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateApprovedOrigin</td>
</tr>
</tbody>
</table>
### Contact flows page

**Contact flows security keys section**

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View contact flow security keys</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:ListSecurityKeys</td>
</tr>
<tr>
<td>Add/remove contact flow security keys</td>
<td>connect:ModifyInstance</td>
</tr>
<tr>
<td></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>Add/remove Lex bots</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>lex:GetBots</td>
</tr>
<tr>
<td></td>
<td>lex:GetBot</td>
</tr>
<tr>
<td></td>
<td>connect:AddLexBots</td>
</tr>
<tr>
<td></td>
<td>connect:RemoveLexBots</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>
<tr>
<td></td>
<td>iam:PutRolePolicy</td>
</tr>
<tr>
<td></td>
<td>iam:AttachRolePolicy</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:RemoveLambdaFunctions</td>
</tr>
<tr>
<td></td>
<td>connect:AddLambdaFunctions</td>
</tr>
<tr>
<td></td>
<td>connect:ListLambdaFunctions</td>
</tr>
<tr>
<td></td>
<td>connect:AssociateLambdaFunction</td>
</tr>
<tr>
<td></td>
<td>connect:DisassociateLambdaFunction</td>
</tr>
<tr>
<td>Action/Use case</td>
<td>Permissions needed</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>lambda:ListFunctions</td>
</tr>
<tr>
<td></td>
<td>lambda:AddPermission</td>
</tr>
<tr>
<td></td>
<td>lambda:RemovePermission</td>
</tr>
</tbody>
</table>

Contact flow logs section

<table>
<thead>
<tr>
<th>Action/Use case</th>
<th>Permissions needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>View contact flow log config</td>
<td>connect:DescribeInstance</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td>Enable/disable contact flow log</td>
<td>connect:ModifyInstance</td>
</tr>
<tr>
<td></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</td>
</tr>
<tr>
<td></td>
<td>connect:DescribeInstanceAttribute</td>
</tr>
<tr>
<td>Update Amazon Polly option</td>
<td>connect:UpdateInstanceAttribute</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>

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 (p. 522)
- Authorization based on Amazon Connect tags (p. 524)
- Amazon Connect IAM roles (p. 524)

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

The Action element of an IAM identity-based policy describes the specific action or actions that will be
allowed or denied by the policy. Policy actions usually have the same name as the associated AWS API
operation. The action is used 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 in
the IAM User Guide.

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
- Contact flow
- Hours of operation
- Phone number
The Resource element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. You specify a resource using an ARN or using the wildcard (*) to indicate that the statement applies to all resources.

The Amazon Connect instance resource has the following ARN:

```
arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}
```

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 in the IAM User Guide. The same article explains with which actions you can specify the ARN of each resource.

**Condition keys**

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.

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.

Provide customers with details about the service-specific condition keys they can use in your service. Include either a list or table of those keys here.
All Amazon EC2 actions support the aws:RequestedRegion and ec2:Region condition keys. For more information, see 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 in the IAM User Guide.

Examples

To view examples of Amazon Connect identity-based policies, see Amazon Connect identity-based policy examples (p. 524).

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 (p. 526).

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 (p. 531).

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 users and roles 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 users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups 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 (p. 525)
- Allow IAM users to view their own permissions (p. 525)
- Grant “View User” permissions (p. 526)
- Describe and update Amazon Connect users based on tags (p. 526)
- Create Amazon Connect users based on tags (p. 527)

Policy best practices

Identity-based policies are very powerful. They 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 Using AWS Managed Policies – To start using Amazon Connect quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get Started Using Permissions With AWS Managed Policies in the IAM User Guide.

- Grant Least Privilege – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant Least Privilege in the IAM User Guide.

- Enable MFA for Sensitive Operations – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using Multi-Factor Authentication (MFA) in AWS in the IAM User Guide.

- Use Policy Conditions for Extra Security – To the extent that it’s practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON Policy Elements: Condition 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": [
```
Grant "View User" permissions

When you create an IAM 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.

```
{
  "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.

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 IAM 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["connect:DescribeUser", "connect:ListUsers"],
      "Resource": "*"
    }
  ]
}
```
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.

```json
{
    "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.

Amazon Connect resource-level policy examples

Amazon Connect supports resource-level permissions for IAM users, so you can specify actions for them for an instance, as shown in the following policies.

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/00dtcddd1-123e-111e-93e3-11111bfbfcc1).

```json
{
    "Version": "2012-10-17",
```

527
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": [  
      "connect:DeleteUser",  
      "connect:UpdateUser*"  
    ],  
    "Resource": "arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/agent/**"  
  }  
]  

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-93e3-11111bfbfcc1/security-profile/11dtcggg1-123e-111e-93e3-11111bfbfcc17 as the parameter for security profile in CreateUser request.

{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "connect:CreateUser"  
      ],  
      "Resource": "*",  
    },  
    {  
      "Effect": "Deny",  
      "Action": [  
        "connect:CreateUser"  
      ],  
    }  
  ]  
}

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.

{  
  "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 contact 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"
        }
    ]
}
```

**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` (p. 530)
- I want to view my access keys (p. 530)
- I'm an administrator and want to allow others to access Amazon Connect (p. 530)
I want to allow people outside of my AWS account to access my Amazon Connect resources (p. 530)

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the iam:PassRole action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies 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 named marymajor tries to use the console to perform an action in Amazon Connect. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

| User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole |

In this case, Mary asks her administrator to update her policies to allow her to perform the iam:PassRole action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

**Important**

Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing Access Keys in the IAM User Guide.

I'm an administrator and want to allow others to access Amazon Connect

To allow others to access Amazon Connect, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon Connect.

To get started right away, see Creating Your First IAM Delegated User and Group in the IAM User Guide.

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 (p. 521).
- 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**

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 Amazon Connect. Service-linked roles are predefined by Amazon Connect 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 easier because you don't have to manually add the necessary permissions. Amazon Connect defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Connect 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 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 named AWSServiceRoleForAmazonConnect – Grants Amazon Connect permission to access AWS resources on your behalf.

The AWSServiceRoleForAmazonConnect service-linked role trusts the following services to assume the role:

- connect.amazonaws.com

The 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 service-link role to access the resources associated with those features:

- **Action:** all Amazon Connect actions, connect:*, on all Amazon Connect resources.
- **Action:** Amazon S3 s3:GetObject, s3:GetObjectAcl, s3:PutObject, s3:PutObjectAcl, 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 Kinesis Data Firehose firehose:DescribeDeliveryStream and firehose:PutRecord, and firehose:PutRecordBatch for the delivery stream defined for Agent event streams and CTRs.
Logging and monitoring Amazon Connect

- Action: Amazon Kinesis Data Streams `kinesis:PutRecord`, `kinesis:PutRecords`, and `kinesis:DescribeStream` for the stream specified for Agent event streams and CTRs.
- Action: Amazon Lex `lex:PostContent` for the bots added to your instance.
- Action: Amazon CloudWatch Logs `logs:CreateLogStream`, `logs:DescribeLogStreams`, and `logs:PutLogEvents` to the CloudWatch Logs group specified for contact flow logging.

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

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.

Editing a Service-Linked Role for Amazon Connect

Amazon Connect does not allow you to edit the AWSServiceRoleForAmazonConnect 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. In the navigation pane of the IAM console, choose Roles.
2. Choose the name of the role to modify.

Deleting a Service-Linked Role for Amazon Connect

You don't need to manually delete the AWSServiceRoleForAmazonConnect 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.

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 (p. 497)
- Logging Amazon Connect API calls with AWS CloudTrail (p. 502)

### Compliance validation in Amazon Connect

Third-party auditors assess the security and compliance of Amazon Connect as part of multiple AWS compliance programs. These include SOC, PCI, HIPAA, CS (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 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 Amazon Connect 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 security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **AWS Config** – This AWS 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 that helps you check your compliance with security industry standards and best practices.

### 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.
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 via 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.
- 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.
- 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. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones 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.

In addition to the AWS global infrastructure, Amazon Connect offers the following features to help support your data resiliency and backup needs:

- Contact flow versioning (p. 173)
- Ability to export your CTR data to Kinesis. This way, you can back up the CTR data across Availability Zones.

To backup call recordings, use the cross-region replication (CRR) feature to copy the call recordings to Amazon S3 buckets in different AWS Regions.

Infrastructure security in Amazon Connect

As a managed service, Amazon Connect is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

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.

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.
Agent training guide for the Amazon Connect CCP

Agents use the Amazon Connect Contact Control Panel (CCP) to interact with customer contacts. It's how they 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://name of your instance.awsapps.com/connect/ccp-v2/

Where name of your instance is provided by your IT department or whoever 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.

We recently released an updated CCP. It provides a single interface for agents to manage both voice and chat contacts. Even if your business is currently taking only voice contacts, we recommend using the updated CCP.

The following image shows the CCP.

Contents
- Training video: How to use the CCP (p. 537)
- Quick start cheat sheet for training agents (p. 537)
- Launch the CCP (p. 538)
- Log in and log out of the Amazon Connect CCP (p. 539)
- Set your status to available (p. 540)
- Chat with contacts (p. 541)
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 outbound calls, transfer calls, accept chat, and more.

Quick start cheat sheet for training agents

The following image shows a one-page cheat sheet to help agents learn the most common tasks in the CCP.
Launch the CCP

The URL to launch the Contact Control Panel (CCP) is:

- **https://name of your instance.awsapps.com/connect/ccp-v2/**

With this updated CCP, your agents can manage both voice and chat contacts 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 (p. 357).
- **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 (p. 361).
- **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 or Firefox for their web browser. For more information, see Grant microphone access in Chrome or Firefox (p. 148).

### 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:

- A link to the CCP. It looks something like this: `https://name of your center.awsapps.com/connect/ccp-v2/`.
- Your agent ID.
- Your agent password.

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**.

   ![Amazon Connect Login Screen](image)

4. If you are prompted to allow access to your microphone and speaker, choose **Allow**.
You're all set to go!

Log out of the Amazon Connect CCP

**Important**
Closing the CCP window 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 Log out agents automatically when they close their CCP (p. 133).

1. At the top of the CCP, select the **Change Status** dropdown menu.
2. Choose **Log out**.

Set your status to available

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.
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 (p. 126). An administrator can specify that up to five chat conversations can be routed to you at the same time.

You can't initiate chat conversations from the CCP.

Customers and agents can't send attachments, such as files, through the chat interface.

**Tip**
Amazon Connect routes contacts to you for only one channel at a time. When you're on a call, you won't be routed a chat conversation. And when you're handling chat conversations, you won't be routed a call.

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.

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.

   ![Available](image)

   Carlos

   ![Accept chat](image)  ![Reject chat](image)

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.

   ![Chat banner](image)
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.
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 each text message.
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 15 seconds. Keep in mind that your admin can't configure this amount of time.

After 15 seconds, the contact is counted as **Agent non-response (p. 442)** 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. This way, with all of your slots occupied, Amazon Connect won't route any more contacts 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**.

**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. You're now doing After Contact Work (ACW) for the customer. Choose Close to end the contact.
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 dial pad and external quick connects (p. 179).

Note the following limitations:

- You can't access agent quick connects while you're on a chat.
- Agents can't receive calls while on a chat.

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, that agent may be handling a chat conversation. They can't receive a call while on a chat.

**Can't see external quick connects in the CCP**

Agent quick connects (p. 179) are not visible in the CCP while you're on a chat.

If you can't see external quick connects (p. 179) in your CCP, however, check that the external quick connect has been added to your queue as described in **Step 2: Enable agents to see quick connects** (p. 180).

**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.
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 (p. 126).

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 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.)

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.
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: Telephony options (p. 86) in Create an Amazon Connect instance (p. 85).

For information about the caller ID that's displayed when you make an outbound call, see Set up outbound caller ID (p. 124).

To make an outbound call

1. In your Contact Control Panel, choose Number pad.
2. Enter the number you want to call and press Call.
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 Check Connectivity Tool (p. 560)
- Common Contact Control Panel (CCP) Issues (p. 560)
- Useful Troubleshooting Tools and Information (p. 561)
- Gathering Helpful Information using the Streams API (p. 562)
- Analyzing the Data (p. 563)
- Validation Testing (p. 563)

Use the Check Connectivity Tool

When your agents are experiencing problems with CCP, we recommend you go to their workstation and run the Amazon Connect Check Connectivity Tool.

This tool checks which web browser the agent is running, and whether the microphone has required permissions. Click the Test buttons to check the ports and latency.

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 allow list entries, not allowing browser microphone access, or not answering your external device. Be sure that you have added to the allow list all IPs covered in the Set up your network (p. 321) 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 allow list. For more information, see the Set up your network (p. 321) 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 (p. 149) 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 (p. 149) 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 (p. 149) 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.

### Useful 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 Trace Record (CTR)**—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 allow list access**—to verify that IP/port ranges are added to the allow list (also known as whitelist) as described in [Set up your network (p. 321)](https://github.com/aws/amazon-connect-streams).

• **Audio capturing and analytic tools**—for latency calculations from the agent's workstation.

• **AWS region latency test tools**—such as the Amazon Connect Call Control Panel Connectivity 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).
Analyzing the Data

The following guidelines can assist you in analyzing the data to identify issues in your environment.

- Use the Contact Trace Record (CTR) / Contact search report to identify the contact IDs for the contacts during which call quality issues occurred. The CTR 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 CTR 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.

- \([\text{overall} \_ \text{latency}]\) is the total latency experienced between caller and agent. This latency can be calculated as \([\text{overall} \_ \text{latency}] = [\text{agent} \_ \text{latency}] + [\text{pstn} \_ \text{latency}]\).
- \([\text{pstn} \_ \text{latency}]\) is the latency between Amazon Connect endpoint and the caller. This latency can be calculated as \([\text{pstn} \_ \text{latency}] = [\text{overall} \_ \text{latency}] - [\text{agent} \_ \text{connection} \_ \text{latency}]\). This latency can be improved by using a different Amazon Connect Region location or avoiding external and circular transfers to geographically distant endpoint locations.
- \([\text{agent} \_ \text{latency}]\) is the latency between Amazon Connect endpoint and the agent. This latency can be calculated as \([\text{agent} \_ \text{latency}] = [\text{overall} \_ \text{latency}] - [\text{recording} \_ \text{latency}]\). 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 \([\text{pstn} \_ \text{latency}]\).
Amazon Connect leverages CloudFront for connectivity. Not all CloudFront ranges are advertised over AWS Direct Connect. This means not all URLs generated by AWS Direct 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].

\[ \text{[agent latency]} = \text{[overall latency]} - \text{[recording latency]} \]

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 (p. 563).
Amazon Connect service quotas

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

- To submit a service quota increase, use the Amazon Connect service quotas increase form. You must be signed in to your AWS account to access the form.
- It can take up to a few days to increase your service quota. If you're increasing your quotas as part of a larger project, be sure to add this time to your plan.
- 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 (p. 97).

<table>
<thead>
<tr>
<th>Item</th>
<th>Default quotas for new accounts created February, 2020 or later. Learn more (p. 568)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lambda functions per instance</td>
<td>35</td>
</tr>
<tr>
<td>Agent status per instance</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>This quota cannot be increased.</td>
</tr>
<tr>
<td>Amazon Connect instances per account</td>
<td>2</td>
</tr>
<tr>
<td>Amazon Lex bots per instance</td>
<td>50</td>
</tr>
<tr>
<td>Concurrent calls per instance</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>If this quota is exceeded, contacts will get a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.</td>
</tr>
</tbody>
</table>

**Tip**

You can calculate your configured quota using CloudWatch metrics. For instructions, see Use CloudWatch metrics to calculate concurrent call quota (p. 502). Or, edit a queue and enter an exceptionally large number for the contact limit. The resulting error message will display your quota. For example, in the following image, it shows the quota for that instance is 99.
<table>
<thead>
<tr>
<th>Item</th>
<th>Default quotas for new accounts created February, 2020 or later. Learn more (p. 568)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent chats per instance</td>
<td>100</td>
</tr>
<tr>
<td>Contact flows per instance</td>
<td>100</td>
</tr>
<tr>
<td>Hours of operation per instance</td>
<td>100</td>
</tr>
<tr>
<td>Phone numbers per instance</td>
<td>5</td>
</tr>
<tr>
<td>Prompts per instance</td>
<td>500</td>
</tr>
<tr>
<td>Queues per instance</td>
<td>50</td>
</tr>
<tr>
<td>Queues per routing profile per instance</td>
<td>50</td>
</tr>
<tr>
<td>Quick connects per instance</td>
<td>100</td>
</tr>
<tr>
<td>Rate of API requests</td>
<td>See Amazon Connect API throttling quotas (p. 569).</td>
</tr>
<tr>
<td>Reports per instance</td>
<td>500</td>
</tr>
<tr>
<td>Routing profiles per instance</td>
<td>100</td>
</tr>
<tr>
<td>Scheduled reports per instance</td>
<td>50</td>
</tr>
<tr>
<td>Security profiles per instance</td>
<td>100</td>
</tr>
</tbody>
</table>

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: BasicQueue-Voice, BasicQueue-Chat, and Queue10-Voice. This counts three towards the service limit of 50.

Routing profile queues
If no queue is added, the agent will only be able to make outbound calls.

<table>
<thead>
<tr>
<th>Name</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>BasicQueue</td>
<td>Voice</td>
</tr>
<tr>
<td>Queue10</td>
<td>Voice</td>
</tr>
</tbody>
</table>
About default quotas

The preceding table provides the default quotas for new Amazon Connect accounts as of February 2020. Because the quotas have been adjusted over time, the quotas in place for your account may be different than the quotas described here.

Feature specifications

The following table lists feature specifications. They cannot be increased.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick connects that can be assigned to a queue</td>
<td>700</td>
</tr>
<tr>
<td>People who can listen in on the same agent call at one time</td>
<td>5</td>
</tr>
<tr>
<td>Contact Trace Record retention</td>
<td>24 months from the time the associated contact was initiated.  You can choose to stream CTRs to Kinesis so you can manage retention and perform advanced analysis.</td>
</tr>
<tr>
<td>Max size of the CTR attributes section</td>
<td>32KB</td>
</tr>
<tr>
<td>Active chats per agent</td>
<td>5</td>
</tr>
<tr>
<td>Total duration per chat</td>
<td>25 hours, including wait time</td>
</tr>
<tr>
<td>Characters per chat message</td>
<td>1024</td>
</tr>
</tbody>
</table>
Countries you can call

You can place calls to the following countries when you create a new instance.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country code allow list for Outbound Calls</td>
<td>Submit a service quota increase request to allow calling to additional countries, or to limit the countries that you can call from. You must be signed in to your AWS account to access the form. For a list of all the countries available for outbound calling, see Amazon Connect pricing.</td>
</tr>
<tr>
<td></td>
<td>Australia</td>
</tr>
<tr>
<td></td>
<td>Canada</td>
</tr>
<tr>
<td></td>
<td>China</td>
</tr>
<tr>
<td></td>
<td>Germany</td>
</tr>
<tr>
<td></td>
<td>Hong Kong</td>
</tr>
<tr>
<td></td>
<td>Israel</td>
</tr>
<tr>
<td></td>
<td>Japan</td>
</tr>
<tr>
<td></td>
<td>Mexico</td>
</tr>
<tr>
<td></td>
<td>Singapore</td>
</tr>
<tr>
<td></td>
<td>Sweden</td>
</tr>
<tr>
<td></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>United Kingdom†</td>
</tr>
</tbody>
</table>

† UK numbers with a 447 prefix are not allowed by default. Before you can dial these UK mobile numbers, you must submit a service quota increase request.

Amazon Connect API throttling quotas

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

- If different IAM 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 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:

- **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.
- **GetTranscript**: a RateLimit of 8 requests per second, and a BurstLimit of 12 requests per second.
- **SendEvent** and **SendMessage**: a RateLimit of 10 requests per second, and a BurstLimit of 15 requests per second.
Additional resources for Amazon Connect

In addition to using the contents of this guide, you can learn more about Amazon Connect by using the online resources listed in this topic.

Amazon Connect Service API documentation

The Amazon Connect Service API Documentation provides details about all the operations, types, inputs and outputs, and error codes.

Amazon Connect Participant Service API

The Amazon Connect Participant Service API provides details about the APIs used by chat participants, such as agents and customers.

Amazon Connect Streams

Use the Amazon Connect Streams documentation 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 SDK and sample implementations

See the Amazon Connect Chat SDK and Sample Implementations for examples of how to enable your app to engage with Amazon Connect chat.
To help you keep track of the ongoing updates and improvements to Amazon Connect, we publish release notices that describe recent changes.

**Updates**

- Upcoming changes (p. 572)
- October 2020 Updates (p. 576)
- September 2020 Updates (p. 577)
- August 2020 Updates (p. 578)
- July 2020 Updates (p. 578)
- June 2020 Updates (p. 579)
- May 2020 Update (p. 580)
- April 2020 Update (p. 580)
- March 2020 Update (p. 580)
- February 2020 Update (p. 581)
- January 2020 Update (p. 581)
- December 2019 Update (p. 582)
- November 2019 Update (p. 582)
- October 2019 Update (p. 583)
- June 2019 Update (p. 583)
- May 2019 Updates (p. 583)
- April 2019 Updates (p. 584)
- March 2019 Update (p. 584)
- February 2019 Updates (p. 585)
- January 2019 Updates (p. 585)
- December 2018 Updates (p. 586)
- November 2018 Updates (p. 587)
- October 2018 Updates (p. 587)
- September 2018 Updates (p. 588)
- August 2018 Updates (p. 588)
- July 2018 Updates (p. 589)
- June 2018 Updates (p. 590)
- April and May 2018 Updates (p. 591)

**Upcoming changes**

We continuously make improvements to Amazon Connect based on your feedback, and also as we find ways to improve your experience. Take a look at this section to learn about planned changes to help improve how your agents work.
New "Next status" for agents

This feature is available only to customers who are using the latest Contact Control Panel (CCP). The URL for the latest CCP looks like this: https://name of your instance.awsapps.com/connect/ccp-v2/

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 will release 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.

The following images of the Contact Control Panel (CCP) show how agents use this feature.

1. The agent is on a contact.
2. The agent chooses their next status, such as Lunch. They can choose only a custom (NPT (p. 447)) 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"

Agents can easily switch from Next status back to Available. The ability to switch their status is useful, for example, if they accidentally choose Next status: Lunch, or if they 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 currently 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 agents status to Offline.

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":
{
"NextAgentStatus": "Lunch"
}
```
"AgentStatus": {
    "ARN": "example-ARN",
    "Name": "Available",
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
},
"NextAgentStatus": {
    "Name": "Lunch",
    "ARN": "example-ARN2",
    "EnqueueTimestamp": "2019-08-13T20:58:00.004Z",
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
}
}

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"**

When we release this feature, it will have the following effect:

- If you integrate with Amazon Connect Streams API and your agents interact directly with the native CCP user interface, then at release 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, then at release 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.

To use **Next status** with a custom CCP integration that does not directly embed the CCP, you will need to make additional changes that will be detailed further in the Amazon Connect Streams README.

**October 2020 Updates**

The following updates were released in October 2020:

**Contact flows**

- Added chat support for whisper flows. For more information, see Contact block: Set whisper flow (p. 253).

**Metrics**

- Released the following real-time metrics:
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 (p. 570)
  - DisconnectParticipant (p. 570)
  - GetTranscript (p. 570)

Contact 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 Amazon Connect Flow language (p. 294).

APIs

Added the following APIs for contact flows:
- CreateContactFlow
- DescribeContactFlow
- UpdateContactFlowContent
- UpdateContactFlowName
August 2020 Updates

The following updates were released in August 2020:

Contact 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 (p. 174).
- Added the ability to select, cut, copy, and paste contact flows. For more information, see Copy and paste contact flows (p. 172).

Telephony

- Added the ability for all customers to enable/disable media support for outbound phone calls. For more information, see Step 3: Telephony options (p. 86) in the Create an Amazon Connect instance (p. 85) 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 (p. 502).

Contact Lens for Amazon Connect

- Updated the security profile permissions for the redaction feature. For more information, see Security profile permissions for Contact Lens (p. 383).

July 2020 Updates

The following updates were released in July 2020:
Contact flows

- The **Set voice** block supports speaking styles with neural text-to-speech (TTS) voices. For more information, see Contact block: Set voice (p. 251).

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 Contact Lens for Amazon Connect (p. 378).

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. For more information, see What's new in metrics (p. 406).
- Corrected how **Occupancy** is calculated. The correct calculation is:

  \[
  \frac{\text{Agent on contact (wall clock time)}}{\text{Agent on contact (wall clock time)} + \text{Agent idle time}}
  \]

June 2020 Updates

The following updates were released in June 2020:

Metrics

- The following historical metrics no longer appear in queue groupings:
  - Agent idle time
  - Agent on contact time
  - Occupancy
- Added upcoming metric changes: new real-time and historical metrics for inbound and outbound contact time. For more information, see What's new in metrics (p. 406).

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.
Amazon Connect Administrator Guide

Contact flows

- 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 (p. 134).
- Published a training video that explains how to use the CCP. For more information, see Training video: How to use the CCP (p. 537).

Contact flows

- The Set disconnect flow block supports voice conversations. For more information, see Contact block: Set disconnect flow (p. 245).
- The Set Voice block supports Amazon Polly Neural Text-to-Speech (NTTS) voices. For more information, see Contact block: Set voice (p. 251).
- The Get queue metrics block can return metrics by channel, for example, by voice or chat. For more information, see Contact block: Get queue metrics (p. 225).

May 2020 Update

The following updates were released in May 2020:

Contact flows

- Added the ability to select multiple blocks at the same time and rearrange them as a group within a contact flow. For more information, see Create an inbound contact flow (p. 171).

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: Telephony options (p. 86) in the Create an Amazon Connect instance (p. 85) topic.
- Added the barge-in-enabled session attribute to the Get customer input (p. 218) block so customers can interrupt Amazon Lex bots with their voice.

March 2020 Update

The following updates were released in March 2020:

Contact flows

- Updated the Store customer input (p. 261) block to allow you to specify a custom terminating keypress.
Metrics

• Announced June 2020: Changes for omnichannel support (p. 408).

Networking

• Updated softphone requirements in Set up your network (p. 321).

February 2020 Update

The following updates were released in February 2020:

Service Quotas

• Adjusted Amazon Connect service quotas (p. 566) for new accounts.

Contact Flows

Updated the following blocks so you can set contact attributes:

• Set customer queue flow (p. 244)
• Set hold flow (p. 247)
• Set whisper flow (p. 253)

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 number (p. 553).
• 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 (p. 321) to include requirements for the updated Contact Control Panel (ccp-v2).

581
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 Contact Lens for Amazon Connect (p. 378).
- Added logging of Amazon Connect API calls with AWS CloudTrail. For more information, see Logging Amazon Connect API calls with AWS CloudTrail (p. 502).

November 2019 Update

The following updates were released in November 2019:

Omnichannel Support

- Added support for chat communications. For more information, see Concepts (p. 8).

Metrics

- For a description of changes, see What's new in metrics (p. 406).

Contact Flows

Added the following contact flow blocks:

- the section called “Wait”
- the section called “Set disconnect flow”

Updated the following contact flow blocks for chat:

- the section called “Play prompt”
- the section called “Get customer input”
- the section called “Store customer input”
- the section called “Set recording and analytics behavior”

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 (p. 509).
Live Media Streaming

- Added that you can capture customer audio for the entire interaction with your contact center. For more information, see Capture customer audio: live media streaming (p. 346).

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 Amazon Connect CCP (p. 536).

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:

Contact Flows

- Added contact 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 (p. 474).

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? (p. 435)

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 (p. 585)
- Contact Flows (p. 585)
- Metrics and Reporting (p. 585)
- Contact Control Panel (CCP) (p. 585)

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.

Contact Flows

- Resolved an issue with the contact 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 trace record (CTR) 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 (p. 586)
- Contact Flows (p. 586)
- Metrics and Reporting (p. 586)

**Contact Routing**
- Resolved an issue where in rare cases agent transfers were failing.

**Contact Flows**
- Resolved an issue where agent transfers were failing.
- Resolved an issue that resulted in periodic delays in publishing contact 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 (p. 586)
- Contact Control Panel (CCP) (p. 586)

**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 trace 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 (p. 587)
- Contact Flows (p. 587)
- Metrics and Reporting (p. 587)

**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.

**Contact Flows**
- Added the new Loop block, which lets you loop through segments of a contact 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 (p. 587)
- Metrics and Reporting (p. 588)
- API (p. 588)

**General**
- Resolved an issue that sometimes resulted in stuck media sessions.
September 2018 Updates

The following updates were released in September 2018:

Updates by category
• General (p. 588)
• API (p. 588)

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 (p. 588)
• Contact Routing (p. 589)
• Metrics and Reporting (p. 589)

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 (p. 589)
- General (p. 589)
- Metrics and Reporting (p. 589)
- Contact Flows (p. 590)

New Features

- Use the Call phone number block to set caller ID (p. 124)
- Add an Amazon Lex bot (p. 332)
- User Management APIs
- Manage contacts in a queue (p. 187)

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.
Contact Flows

- Added drop-down menus for contact attributes to make it easier to reference attributes in a contact flows.

June 2018 Updates

The following updates were released in June 2018:

**Updates by category**
- General (p. 590)
- Telephony and Voice (p. 590)
- Contact Flows (p. 590)
- Metrics and Reporting (p. 590)
- Contact Control Panel (CCP) (p. 591)

**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.

**Contact Flows**

- Renamed the *Set queue* block to *Set working queue*.
- Added a *Copy to clipboard* button next to the ARN of a contact flow so you can easily copy the ARN. Choose *Show additional flow information* under the name of the contact 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 *Use the Call phone number block to set caller ID* (p. 124).
- Released contact attributes for system metrics, including a new *Get metrics* block in contact flows. For more information, see *How to use system metric attributes* (p. 284).

**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 (p. 591)
- Telephony and Voice (p. 591)
- Contact Flows (p. 591)
- Metrics and Reporting (p. 592)
- Contact Control Panel (CCP) (p. 592)

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 contact 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.

Contact Flows

- Resolved an issue with publishing a contact flow in the case where an AWS Lambda function block is used in a contact flow, and the input type for a parameter was changed from Send attribute with a System attribute is changed to Send text. These contact 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 into 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.
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 (p. 88).
- Your region.
- A detailed description of the issue.
# Document history

The following table describes important changes in each release of the CloudWatch Events User Guide, beginning in June 2018. For notification about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service quotas (p. 594)</td>
<td>Noted that up to 700 quick connects can be added to a queue. See Feature specifications.</td>
<td>October 5, 2020</td>
</tr>
<tr>
<td>Security (p. 594)</td>
<td>Added new topic on Required permissions for managing access to the Amazon Connect console.</td>
<td>September 24, 2020</td>
</tr>
<tr>
<td>Service quotas (p. 594)</td>
<td>Updated the service quotas for the following Amazon Connect Participant Service APIs: CreateParticipantConnection, DisconnectParticipant, and GetTranscript. For more information, see Amazon Connect Participant Service API throttling quotas.</td>
<td>September 22, 2020</td>
</tr>
<tr>
<td>Show agent queues in a Queues table. (p. 594)</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 Show agent queues in a Queues table.</td>
<td>September 18, 2020</td>
</tr>
<tr>
<td>Migrate contact flows to a different instance (p. 594)</td>
<td>You can migrate hundreds of contact flows using a set of contact flow APIs. For more information, see Migrate contact flows to a different instance.</td>
<td>September 18, 2020</td>
</tr>
<tr>
<td>Languages supported by Amazon Connect (p. 594)</td>
<td>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.</td>
<td>September 18, 2020</td>
</tr>
<tr>
<td>Amazon Connect Flow language (p. 594)</td>
<td>You can use the Amazon Connect Flow language to efficiently update contact flows that you’re migrating from one</td>
<td>September 18, 2020</td>
</tr>
</tbody>
</table>
Earlier updates

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added topic on setting up agent-to-agent transfers.</td>
<td>For more information, see Set up agent-to-agent transfers (p. 183).</td>
<td>August 19, 2020</td>
</tr>
<tr>
<td>Added section on requirements for custom termination points.</td>
<td>For more information, see Request international numbers, special numbers, or termination points (p. 96).</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 (p. 146).</td>
<td>For more information, see I use the Amazon Connect Streams API (p. 146).</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 Monitor metrics and run reports (p. 406).</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 (p. 408).</td>
<td>July 8, 2020</td>
</tr>
<tr>
<td>Updated the Set disconnect flow (p. 245) block, which now supports voice conversations.</td>
<td>For more information, see Set disconnect flow (p. 245).</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 What's new in metrics (p. 406).</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 (p. 134).</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 (p. 537).</td>
<td>June 16, 2020</td>
</tr>
<tr>
<td>Deprecated metrics: Agent on contact time, Agent idle time, Occupancy.</td>
<td>For more information, see June 2020: Changes for omnichannel support (p. 408).</td>
<td>June 12, 2020</td>
</tr>
<tr>
<td>Added topic on quick connects work</td>
<td>For more information, see How quick connects work (p. 181).</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 Get administrative support for Amazon Connect (p. 593) and About inherited permissions (p. 362).</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 Log out agents automatically when they close their CCP (p. 133).</td>
<td>April 16, 2020</td>
</tr>
<tr>
<td>Updated the Get customer input block to support timeout values for voice input</td>
<td>For more information, see Get customer input (p. 218).</td>
<td>April 8, 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 terminating keypress</td>
<td>For more information, see Store customer input (p. 261).</td>
<td>March 31, 2020</td>
</tr>
<tr>
<td>Added NLB endpoints and required domain for softphones</td>
<td>For more information, see Set up your network (p. 321).</td>
<td>March 23, 2020</td>
</tr>
<tr>
<td>Announced upcoming changes for metrics</td>
<td>For more information, see June 2020: Changes for omnichannel support (p. 408).</td>
<td>March 23, 2020</td>
</tr>
<tr>
<td>Added topic on region requirements for phone numbers</td>
<td>For more information, see Region requirements for phone numbers (p. 103).</td>
<td>March 11, 2020</td>
</tr>
<tr>
<td>Added tutorials</td>
<td>For more information, see Tutorials: An introduction to Amazon Connect (p. 25).</td>
<td>March 6, 2020</td>
</tr>
<tr>
<td>Added topic on tracking who deleted recordings</td>
<td>For more information, see Track who deleted or listened to recordings (p. 373).</td>
<td>March 5, 2020</td>
</tr>
<tr>
<td>Added topic on emergency admin access</td>
<td>For more information, see Emergency admin login (p. 92).</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 (p. 422), Share custom reports (p. 424), View a shared report (p. 425), and Publish reports (p. 426).</td>
<td>January 22, 2020</td>
</tr>
<tr>
<td>Updated contact 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 (p. 417).</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 (p. 321).</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 (p. 502).</td>
<td>December 13, 2019</td>
</tr>
<tr>
<td>Added a section on analyzing conversations</td>
<td>For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 378).</td>
<td>December 02, 2019</td>
</tr>
<tr>
<td>Added information about live media streaming</td>
<td>For more information, see Capture customer audio: live media streaming (p. 346).</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 Chat (p. 11). Also added these topics: Best practices for Amazon Connect (p. 22), About agent status (p. 414), About contact states (p. 415), and Additional resources for Amazon Connect (p. 571).</td>
<td>November 21, 2019</td>
</tr>
<tr>
<td>Added topic on using IAM</td>
<td>For more information, see Identity and access management for Amazon Connect (p. 509).</td>
<td>November 14, 2019</td>
</tr>
<tr>
<td>Added dimensions</td>
<td>Added dimensions to the Amazon Connect metrics sent to CloudWatch. See Monitoring your instance using CloudWatch (p. 497).</td>
<td>October 22, 2019</td>
</tr>
<tr>
<td>Added a networking topic</td>
<td>Consolidated networking content into Set up your network (p. 321). 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>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 contact flow after the call with the external party ends. For more information, see Resume a contact flow after transfer (p. 186).</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 Capture customer audio: live media streaming (p. 346).</td>
<td>December 21, 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 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 (p. 188).</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 (p. 101).</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 (p. 477).</td>
<td>October 30, 2018</td>
</tr>
<tr>
<td>Added troubleshooting and best practices</td>
<td>Troubleshooting Issues with the Contact Control Panel (CCP) (p. 560) 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 Use Service-Linked Roles for Amazon Connect (p. 531).</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 Transfer to queue block to enable transferring calls that are already in a queue to another queue. For more information, see Manage contacts in a queue (p. 187).</td>
<td>July 31, 2018</td>
</tr>
<tr>
<td>Added information about the Call phone number block</td>
<td>Updated the content about contact flows to include the new Call phone number block, including how to use the block in a contact flow. For more information, see Use the Call phone number block to set caller ID (p. 124).</td>
<td>July 2, 1018</td>
</tr>
<tr>
<td>Added information about contact attributes and the Get queue metrics block</td>
<td>For more information, see Use Amazon Connect contact attributes (p. 276).</td>
<td>June 18, 2018</td>
</tr>
<tr>
<td>Added information about new metrics sent to Amazon CloudWatch Logs.</td>
<td>Monitoring your instance using CloudWatch (p. 497) 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 Configure SAML with IAM for Amazon Connect (p. 75).</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 Monitor live conversations (p. 367).</td>
<td>December 10, 2017</td>
</tr>
<tr>
<td>Added information about contact flow logs</td>
<td>For more information, see Enable contact flow logs (p. 199).</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about contact flow import/export</td>
<td>For more information, see Import/export contact flows (p. 197).</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about agent event streams</td>
<td>For more information, see Amazon Connect agent event streams (p. 474).</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 Port your current phone number (p. 97).</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Added information about Login/Logout reports</td>
<td>For more information, see Login/Logout reports (p. 470).</td>
<td>November 1, 2017</td>
</tr>
<tr>
<td>Initial release</td>
<td>Initial release of the Amazon Connect Administrator Guide.</td>
<td>March 28, 2017</td>
</tr>
</tbody>
</table>