Amazon Connect: Administrator Guide
Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

What Is Amazon Connect? ....................................................................................................................... 1  
Features of Amazon Connect .................................................................................................................. 1  
Supported Browsers ............................................................................................................................. 1  
Related Services .................................................................................................................................... 2  
Get Started ............................................................................................................................................... 4  
Prerequisites ............................................................................................................................................ 4  
Step 1: Identity Management .................................................................................................................. 4  
Step 2: Administrator .............................................................................................................................. 5  
Step 3: Telephony Options ...................................................................................................................... 5  
Step 4: Data Storage ............................................................................................................................... 5  
Step 5: Review and Create ...................................................................................................................... 6  
Next Steps ............................................................................................................................................... 6  
Contact Centers ...................................................................................................................................... 7  
Instances .................................................................................................................................................. 7  
Create an Instance .................................................................................................................................... 7  
Update Instance Settings ......................................................................................................................... 7  
Manage Users ........................................................................................................................................... 8  
Enable Data Streaming ............................................................................................................................. 9  
Integrate with Your CRM ....................................................................................................................... 9  
Log in as Administrator ............................................................................................................................ 9  
Delete Your Instance ............................................................................................................................... 10  
Phone Numbers ....................................................................................................................................... 10  
Claim a Phone Number .......................................................................................................................... 10  
Associate a Phone Number with a Contact Flow ................................................................................ 11  
Port Your Current Phone Number ......................................................................................................... 11  
Phone Numbers for Asia Pacific (Tokyo) ............................................................................................... 13  
Agents ..................................................................................................................................................... 15  
Agent Hierarchies ..................................................................................................................................... 16  
Agent Status ............................................................................................................................................. 16  
Queues ..................................................................................................................................................... 17  
Set the Hours of Operation ...................................................................................................................... 17  
Create a Queue ......................................................................................................................................... 18  
Create a Routing Profile ......................................................................................................................... 18  
Contact Flows ......................................................................................................................................... 19  
Contact Flow Templates ......................................................................................................................... 20  
Add Security Keys ..................................................................................................................................... 20  
Create a Contact Flow ............................................................................................................................. 21  
Create Prompts .......................................................................................................................................... 22  
Add Text-to-Speech ............................................................................................................................... 22  
Create Quick Connects .......................................................................................................................... 23  
Add an Amazon Lex Bot ........................................................................................................................ 24  
Resume a Contact Flow After Transfer ............................................................................................... 24  
Initiate an Outbound Call ......................................................................................................................... 26  
Manage Calls in a Queue ........................................................................................................................ 27  
Transfer Calls Directly to a Specific Agent ............................................................................................ 28  
Contact Block Definitions ...................................................................................................................... 30  
Lambda Functions ..................................................................................................................................... 36  
Live Media Streaming ............................................................................................................................. 40  
Contact Attributes ..................................................................................................................................... 46  
Contact Flow Import/Export ................................................................................................................ 62  
Contact Control Panel ........................................................................................................................... 65  
Amazon Connect CCP Concepts ............................................................................................................ 65  
Access the Amazon Connect CCP ........................................................................................................ 65  
Grant Microphone Access ..................................................................................................................... 66
<table>
<thead>
<tr>
<th>Update Date</th>
<th>Section Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2018 Updates</td>
<td>Contact Flows</td>
<td>138</td>
</tr>
<tr>
<td></td>
<td>Metrics and Reporting</td>
<td>139</td>
</tr>
<tr>
<td>September 2018 Updates</td>
<td>General</td>
<td>139</td>
</tr>
<tr>
<td></td>
<td>API</td>
<td>139</td>
</tr>
<tr>
<td>August 2018 Updates</td>
<td>General</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Contact Routing</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Metrics and Reporting</td>
<td>140</td>
</tr>
<tr>
<td>July 2018 Updates</td>
<td>New Features</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>General</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Metrics and Reporting</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Contact Flows</td>
<td>141</td>
</tr>
<tr>
<td>June 2018 Updates</td>
<td>General</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Telephony and Voice</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Contact Flows</td>
<td>142</td>
</tr>
<tr>
<td></td>
<td>Metrics and Reporting</td>
<td>142</td>
</tr>
<tr>
<td></td>
<td>Contact Control Panel (CCP)</td>
<td>142</td>
</tr>
<tr>
<td>April and May 2018 Updates</td>
<td>General</td>
<td>142</td>
</tr>
<tr>
<td></td>
<td>Telephony and Voice</td>
<td>142</td>
</tr>
<tr>
<td></td>
<td>Contact Flows</td>
<td>143</td>
</tr>
<tr>
<td></td>
<td>Metrics and Reporting</td>
<td>143</td>
</tr>
<tr>
<td></td>
<td>Contact Control Panel (CCP)</td>
<td>143</td>
</tr>
<tr>
<td>Document History</td>
<td></td>
<td>144</td>
</tr>
</tbody>
</table>
What Is Amazon Connect?

Amazon Connect is a cloud-based contact center solution. Amazon Connect makes it easy to set up and manage a customer contact center and provide reliable customer engagement at any scale. You can set up a contact center in just a few steps, add agents from anywhere, and start to engage with your customers right away.

Amazon Connect provides rich metrics and real-time reporting that allow you to optimize contact routing. You can also resolve customer issues more efficiently by putting customers in touch with the right agents. Amazon Connect integrates with your existing systems and business applications to provide visibility and insight into all of your customer interactions. Amazon Connect requires no long-term contracts, and you pay only for what you use.

Features of Amazon Connect

- **Amazon Connect instance**—A virtual contact center based in the AWS cloud. Instances can scale to support any size of business.
- **User administration**—Add users and configure them with permissions that are appropriate to their roles (for example, agents or managers. You can authenticate users through Amazon Connect, an existing AWS Directory Service directory service, or a SAML-based identity provider (IdP).
- **Contact Control Panel (CCP)**—The client interface used by agents to handle customer contacts.
- **Contact flows**—Defines the customer experience with the contact center from start to end. For example, you can play prompts, get input from the customer, branch based on customer impact, invoke a Lambda function, or integrate an Amazon Lex bot.
- **Skills-based routing**—Contacts can be routed based on the skills required of the agents.
- **Metrics and reporting**—Real-time and historical information about the activity in your contact center.

Supported Browsers

Before you start working with Amazon Connect, use the following table to verify that your browser is supported.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>Check your version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest 3 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 3 versions</td>
<td>Open Firefox. On the menu, choose the Help icon and then choose About Firefox. The version number is listed underneath the Firefox name.</td>
</tr>
</tbody>
</table>
Related Services

The following services are used with Amazon Connect:

- **AWS Directory Service**—AWS Directory Service for Microsoft Active Directory (Enterprise Edition) enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. Amazon Connect user and identity management is based on this service.

- **Amazon S3**—Amazon Connect uses Amazon Simple Storage Service (Amazon S3) to store data from Amazon Connect, such as call recordings and metrics reports.

- **AWS Lambda**—Lambda allows you to build and run code quickly without provisioning or managing servers. In Amazon Connect, you can invoke functions in a contact flow. You can build Lambda functions that communicate with your internal systems, such as retrieving the status of an order. You can then use the values returned from the function in your contact flows to personalize the customer experience.

- **Amazon Lex**—Amazon Connect integrates with Amazon Lex to provide conversational interfaces using voice and text. Amazon Lex provides automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the customer intent. For more information, see the Amazon Lex Developer Guide.

- **Kinesis**—Amazon Connect integrates with Kinesis as the platform for streaming contact trace records (CTR) and agent event streams data. The data is published to Kinesis in JSON format, and include details about contacts and agent activities in your contact center. You can then enable detailed analysis and reporting on your contact center data. You can use Amazon QuickSight (a cloud-powered business analytics service) or your own BI tools to build powerful visualizations on top of synthesized data. Additionally, this data can be streamed to Elasticsearch to query on this data using a convenient visual interface. For more information, see the Amazon Kinesis Data Streams Developer Guide.

  **Note**
  
  Amazon Connect does not support publishing data to streams for which server-side encryption is enabled.

- **Amazon CloudWatch**—Amazon Connect integrates with CloudWatch to provide you with real-time operational metrics for your contact center. Metrics include total calls per second, calls rejected and throttled, percentage of concurrent calls, failed / missed calls count (errors, bad number/address, busy/line engaged), and contact flow errors. You can set up monitors on these metrics in order to stay on top of the health of your contact center. For more information, see CloudWatch Metrics for Your Amazon Connect Instance (p. 100).

- **AWS Identity and Access Management**—The AWS Management Console requires your user name and password to determine whether you have permission to access its resources. You should not use root credentials to access AWS because root user credentials cannot be revoked or limited in any way. Instead, we recommend that you create an IAM user and add the user to an IAM group with administrative permissions. You can then access the console using the IAM user credentials. For more information, see the IAM User Guide.

  If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. For more information, see Create Individual IAM Users in the IAM User Guide.
• **AWS Key Management Service**—Amazon Connect is integrated with AWS KMS to protect your customer data. Key management can be performed from the AWS KMS console. For more information, see *What is the AWS Key Management Service* in the *AWS Key Management Service Developer Guide*. 
Get Started with Amazon Connect

To get started with Amazon Connect, create an Amazon Connect virtual contact center instance. An instance contains the configuration, data, and artifacts for your contact center. To enable features for your contact center, you modify the settings for your instance.

Tasks
- Prerequisites (p. 4)
- Step 1: Identity Management (p. 4)
- Step 2: Administrator (p. 5)
- Step 3: Telephony Options (p. 5)
- Step 4: Data Storage (p. 5)
- Step 5: Review and Create (p. 6)
- Next Steps (p. 6)

Prerequisites

- 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.

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 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.
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

Customers can call into your contact center and speak to an agent. Agents can use the web-based softphone provided by Amazon Connect for incoming and outgoing telephony, or agents can use a desk phone through the public switched telephone network (PSTN).

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. Choose Next step.

Step 4: Data Storage

Data, such as call recordings and reports, is stored securely in an Amazon S3 bucket. When you create an instance, by default, we create a bucket and encrypt it using AWS Key Management Service. This bucket and key are used for both calling recordings and exported reports. Alternatively, you can specify separate buckets and keys for call recordings and exported reports.

By default, we enable contact flow logs. For more information, see Contact Flow Logs (p. 97).

You can choose Next step to keep the default data storage settings, or you can customize them as follows.

To customize the data storage settings for your instance

1. Choose Customize settings.
2. (Optional) To specify the bucket and KMS key for call recordings, 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 exported reports, choose Exported reports, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
4. (Optional) To disable contact flow logs, clear Enable Contact flow logs.
5. 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. 6).

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 edit its settings, such as telephony, data storage, and data streaming. You can assign your contact center a phone number or import your own phone number. You can add agents, managers, and operators 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. You can define the experience that your customers have with your contact center using contact flows. You can generate metrics reports to monitor your contact center, including efficiency, utilization, and agent performance. For more information, see the following resources.

Resources

- Instance Settings (p. 7)
- Phone Numbers (p. 10)
- Agents (p. 15)
- Queues (p. 17)
- Contact Flows (p. 19)
- Metrics Reports (p. 103)
Amazon Connect Contact Centers

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. 4).

After you create an instance, you can edit its settings, such as telephony, data storage, and data streaming. 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. You can define the experience that your customers have with your contact center using contact flows.

Contents
- Amazon Connect Instances (p. 7)
- Phone Numbers for Your Contact Centers (p. 10)
- Amazon Connect Agents (p. 15)
- Amazon Connect Queues (p. 17)
- Amazon Connect Contact Flows (p. 19)

Amazon Connect Instances

To create an Amazon Connect contact center, you create an virtual contact center instance. Each instance contains all the resources and settings related to your contact center. You can manage settings for your instance from the Amazon Connect console. You can manage settings for your contact center from within your contact center instance.

You can create multiple instances, but each instance functions only within the AWS Region in which you create it. Settings, users, metrics, and reporting are not shared between instances.

Contents
- Create an Instance (p. 7)
- Update Instance Settings (p. 7)
- Manage Users (p. 8)
- Enable Data Streaming (p. 9)
- Integrate with Your CRM (p. 9)
- Log in as Administrator (p. 9)
- Delete Your Instance (p. 10)

Create an Instance

To create a contact center instance, see Get Started with Amazon Connect (p. 4).

Update Instance Settings

To update the instance settings, open the Amazon Connect console, choose the name of the instance from Instance Alias, and complete the following procedures.
To update the 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. Choose **Save**.

To update the data storage settings
1. In the navigation pane, choose **Data storage**.
2. (Optional) To specify the bucket and KMS key for call recordings, choose **Call recordings**, **Edit**, specify the bucket name and prefix, select the KMS key by name, and then choose **Save**.
3. (Optional) To enable live media streaming, choose **Live media streaming**, **Edit**. For more information, see **Live Media Streaming in Contact Flows** (p. 40).
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**.

To enable data streaming
1. In the navigation pane, choose **Data streaming**.
2. Choose **Enable data streaming**. For more information, see **Enable Data Streaming** (p. 9).
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**.

To update the 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 **Add Security Keys** (p. 20).
3. (Optional) To integrate with Amazon Lex, select a Lex bot. For more information, see **Add an Amazon Lex Bot** (p. 24).
4. (Optional) To integrate with AWS Lambda, select a Lambda function. For more information, see **Lambda Functions in Contact Flows** (p. 36).
5. (Optional) To enable contact flow logs, choose **Enable contact flow logs**. For more information, see **Contact Flow Logs** (p. 97).

Manage Users

You can add users and configure them with permissions that are appropriate to their roles (for example, agents or managers). For more information, see **Amazon Connect Security Profiles** (p. 80). Contacts can be routed based on the skills required of the agents. For more information, see **Create a Routing Profile** (p. 18).
To add 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. 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.

To update 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 checkbox for one or more users and choose Edit.
4. (Optional) To reset the password, choose reset password. Specify a new password and then choose Submit.
5. (Optional) Choose a routing profile.
6. (Optional) Add or remove security profiles.
7. (Optional) Update the agent hierarchy.
8. Choose Save.

Enable Data Streaming
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.

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, enable encryption for call recordings or scheduled reports, create a customer master key (CMK) to use for encryption, and then choose the same CMK for the Kinesis data stream that you use for call recording or scheduled reports. For more information, see Creating Keys in the AWS Key Management Service Developer Guide.

Integrate with Your CRM
You can integrate Amazon Connect with the Salesforce and Zendesk CRMs. 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 Contact Streams. When completed, add the origin URLs to your instance settings. This enables communication between Amazon Connect and your CRM. For more information, see Application Integration (p. 68).

Log in as Administrator
A user assigned to the Admin security profile can log in to the instance with full administrator permissions from the Amazon Connect console. This can be helpful if you forget the password for the administrator account. Users assigned to other security profiles, such as Agent, don't have the permissions required to log in with administrator permissions.
To log in with administrator permissions

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 Overview.
4. Choose Log in as administrator.
5. When prompted, enter your password and choose Sign In.

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. You lose all settings, data, metrics, and reports associated with the instance.

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.

Phone Numbers for Your Contact Centers

After you create an Amazon Connect instance, you can claim a phone number to use for your contact center. After you claim a number, you can place a test call in to your contact center to confirm that it is working correctly. If you want to keep a phone number you already have, you can port the phone number and use it with Amazon Connect.

Agents handle calls using the Contact Control Panel (CCP). For more information, see Amazon Connect Contact Control Panel (p. 65).

Contents

- Claim a Phone Number (p. 10)
- Associate a Phone Number with a Contact Flow (p. 11)
- Port Your Current Phone Number (p. 11)
- Phone Numbers for Amazon Connect in the Asia Pacific (Tokyo) Region (p. 13)

Claim a Phone Number

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
   If you select a country, but there are no numbers displayed for that country, you can request 
   additional numbers for the country using the Amazon Connect service limits increase form.
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 limit of 10 phone numbers per Amazon Connect instance. If you reach your limit, 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 than 10 phone numbers, you can request a 
service limit increase using the Amazon Connect service limits increase form.

**Associate a Phone Number with a Contact Flow**

You can attach contact flows to phone numbers. You cannot assign a contact flow to a phone number 
until the contact flow is published.

**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. Select the number to edit, expand Contact flow / IVR, and select the contact flow.
5. Choose Save.

**Port Your Current Phone Number**

To continue to use your current United States 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.

Porting phone numbers typically takes between two to four weeks after you submit the required 
information. The amount of time depends on the complexity of the request and your current carrier. 
Porting toll-free numbers, or requests to port a large quantity of numbers at one time, usually take 
longer than porting local, direct dial numbers.

We recommend that you select a phone number for Amazon Connect so that you can become familiar 
with the service while waiting for your number to be ported.

**To port your current phone number to Amazon Connect**

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Log in with the account used to create the Amazon Connect instance to which to port your current 
   number.
4. On the Support Center page, choose Create Case.
5. Fill in values for the following fields:
   - For Regarding, choose Service Limit Increase.
• For **Limit Type**, choose **Connect**.
• For **Region**, select the Region in which you created your Amazon Connect instance.
• For **Limit**, choose **Phone Number Porting**.
• For **New limit value**, enter the number of phone numbers to port.
• For **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 do not know all of these details, you may leave information out.

6. Fill in the rest of the form, and choose **Submit**.

### About Porting Phone Numbers

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

We collect the information necessary to verify that you are authorized to port the numbers that you request. We pass that information on to your existing carrier, and coordinate with the new carrier to get your number ported. Each carrier has their own process and requirements for number porting. Your number cannot be ported until your current carrier verifies that you own and are authorized to port the numbers requested. Your current carrier must approve the request to port your number before the new carrier can provision the number. After that is complete, the Amazon Connect team can start configuring your Amazon Connect instance to use the ported numbers.

The steps in the porting process are as follows:

1. Submit a support ticket to port your number.
2. Confirm number portability. The Amazon Connect team confirms 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.
3. Complete the Letter of Authorization/Agency (LOA). When you complete the LOA form, the information you provide must match the information on file with your current carrier. If the information does not match, it may delay the porting of your number. The LOA form authorizes your current carrier to release your number and allow it to be ported. If your number can be ported, we provide you with an LOA form appropriate for the type of number to port. There are different forms for local, Direct Inward Dial (DID), and toll-free numbers. If you are porting multiple numbers from different carriers, fill out a separate form for each carrier.

On the LOA form, include the following:

- 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

4. To get the port started, the Amazon Connect team submits the LOA to the carrier for Amazon Connect on your behalf. The new carrier works with your current carrier to move your current number over to their service. This step typically takes 3–5 business days.

   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.

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.
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>
</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 limits increase form to request an 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 limit 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 limit 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/.
   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 limits 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, with an address visible on the document that matches the city from which the phone
    number is assigned.
  - 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 resolves the
ticket, and address validation is confirmed you can then follow step 6 above to claim a Tokyo 03 prefix
number.

Amazon Connect 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.
Agent Hierarchies

You can organize agents and teams into groups 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. The hierarchies are reflected in reports and historical metrics to allow for granulated reporting. Here are a couple of things to note about using hierarchies:

- Removing agents from a level affects historical reporting.
- Hierarchies do not determine agent permissions or security settings. They define the organizational structure of agent groups for effective reporting.

To manage who can create hierarchies and see the location and skill set data, create a security profile and then grant the appropriate permissions to users assigned to that profile. For more information, see Amazon Connect Security Profiles (p. 80).

**To configure a new agent hierarchy**

1. Choose Contact management, Agent hierarchy.
2. Enter a name and choose + to create the first level of your hierarchy.
3. Choose + to add more levels to your hierarchy.
4. Choose Save to apply the changes, or Cancel to undo them.

When a hierarchy has been created, you can add groups, teams, and agents from the top down.

**To add groupings to a hierarchy**

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.

Agent Status

Agent status is used for reporting and metrics, as well as resource management. Amazon Connect provides default editable states, but custom status values can be added. Customized agent status values are auxiliary by default.

**To add a new agent status**

1. Choose Contact management, Agent status, Add new agent status.
2. Enter a status name, description, and type, and select whether the status should be enabled in the CCP.
3. Choose Save.
To edit a status
1. Choose Contact management, Agent status.
2. Hover over the status name and choose the pencil icon.
3. Enter the new information, and choose Save to apply the changes.

Choose View Historical Changes to view the change history. You can filter changes by date (between two dates) or by user name. If you cannot see the View historical changes link, ensure that you have the proper permissions to view these changes.

Amazon Connect Queues

A queue is ‘waiting area’ that holds contacts to be answered by agents. You can use a single queue to handle all incoming contacts, or you can set up queues mapped to agents with specific skill sets.

Contacts are routed through your contact center based on the routing logic you define in your contact flows. You can also use routing profiles to manage how agents are allocated to queues, such as routing specific types of contacts to agents with specific skill sets. If no agent with the required skill set is available, the contact is placed in the queue you define in the contact flow.

Calls in a queue are automatically prioritized and forwarded to the next available agent. Customers 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 call 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.

Use the metrics and reporting features of Amazon Connect to monitor queue performance and wait times in your in your contact center to optimize agent efficiency and reduce customer hold times. Make sure to plan for peak busy times and how additional calls are handled when your contact center is at full call capacity. To learn more about queue metrics, see Amazon Connect Metrics and Contact Trace Records (p. 103). To learn more about using queue metric attributes in contact flows, see Using System Metric Attributes (p. 56).

Queue metrics can be monitored and reviewed using both real-time and historical metrics.

Set the Hours of Operation

Hours of operation define when a queue is available, and may be referenced in contact flows. Hours of operation are a required component when setting up queues, and must be completed first.

To add hours of operation in the console
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.
Create a Queue

When you create a queue, it is automatically active and can be assigned to a routing profile. Users with the proper permissions can deactivate the queue, which puts it in an offline mode and makes it unavailable to assign to a routing profile.

When you create a queue, you can specify an **Outbound caller ID name** and **Outbound caller ID number**. You can also provide a phone number in a **Set callback number** block in a contact flow. The callback name and number is sent as the origination party when Amazon Connect initiates the call to the destination. However, the information displayed to the person called may not always match the name or number set during call initiation. In some cases, the callback name is provided by the carrier of the person you are calling. The information may not be up-to-date with that carrier, or the number may get passed differently between systems due to hardware or configuration differences. If this is the case, the person that you call may not see the phone number, or may see the name of a previously registered owner of the number, instead of the name of the registered person from your organization.

**To create a queue**

1. Choose **Routing, Queues, Add new queue**.
2. Add the appropriate information about your queue and choose **Add new queue**.

**To edit a queue**

1. Choose **Routing, Queues**, and select the queue to edit.
2. Edit the queue details as required.
3. Choose **Save**.

**To disable an active queue**

1. Choose **Routing, Queues**.
2. Hover over the name of the queue to edit and choose the power icon.
3. Choose **Disable**.

Create a Routing Profile

A routing profile is a collection of queues that determines how contacts are routed to agents. Routing profiles are used to prioritize contacts across specific queues and manage the priority in which contacts are handled based on the queues they are routed to. Routing profiles are managed and assigned to agents by the administrator. An agent can only be assigned a single routing profile at a time; however, they may serve multiple queues, based on rules defined in the routing profile.

**To create a routing profile**

1. Choose **Users, Routing profiles, Add new profile**.
2. Enter or choose the following information:
   - **Name**—A searchable display name.
   - **Description**—The routing profile's function.
   - **Routing profile queues**—A queue to associate with the routing profile. You can add multiple queues.
   - **Priority**—The order in which contacts are handled by the queue they are in. Set values in order of importance, with the lowest number equaling the highest priority. 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.
Example Routing Profile

The following is an example routing profile.

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

This profile prioritizes Premium Support 1 and Premium Support 2 equally (because each has a priority 1).

- Agents with this profile may take calls for Premium Support 3 when customers for Premium Support 3 are waiting for 20 seconds or longer (and no Premium Support 1 or Premium Support 2 calls are in queue).
- Agents with this profile may take calls for Premium Support 4 when customers for Premium Support 4 are waiting 80 seconds or longer (and no calls for Premium Support 1, Premium Support 2 or Premium Support 3 are in queue).

Amazon Connect Contact Flows

A contact flow defines the customer experience with a contact center from start to finish. You can configure your contact flows using the AWS Management Console. You can use the contact flow templates provided or create your own contact flows from scratch.

Contents

- Contact Flow Templates (p. 20)
- Add Security Keys (p. 20)
- Create a Contact Flow (p. 21)
- Create Prompts (p. 22)
- Add Text-to-Speech (p. 22)
- Create Quick Connects (p. 23)
- Add an Amazon Lex Bot (p. 24)
- Resume a Contact Flow After Transfer (p. 24)
- Initiate an Outbound Call (p. 26)
- Manage Calls in a Queue (p. 27)
- Transfer Calls Directly to a Specific Agent (p. 28)
- Contact Block Definitions (p. 30)
- Lambda Functions in Contact Flows (p. 36)
Contact Flow Templates

The following contact flow templates are available:

- **Customer queue flow**—Manages 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.

- **Customer hold flow**—Manages 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.

- **Customer whisper flow**—Manages 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.

- **Outbound whisper flow**—Manages 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 call recording behavior block.

- **Agent hold flow**—Manages 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.

- **Agent whisper flow**—Manages 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.

- **Transfer to agent flow**—Manages 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.

- **Transfer to queue flow**—Manages 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.

Add Security Keys

Amazon Connect can encrypt sensitive data collected by contact flows using public-key cryptography. Provide an X.509 certificate within your contact flow to encrypt data captured using the stored customer input system attribute. You must upload a signing key in .pem format in order to use this feature. The signing 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.

Data that is encrypted within a contact flow is made available through the stored customer input system attribute. The AWS Encryption SDK can be used to decrypt this data within your system. For more information, see the AWS Encryption SDK Developer Guide.

**To add a security key**

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. Choose **Add key**.
5. Paste the contents of your public key in **Public key contents** and choose **Add**.

**Create a Contact Flow**

You can create a variety of contact flows in Amazon Connect, such as transfer flows. The starting point for all contact flows is the contact flow designer. You can make your contact flows as simple or complex as needed.

**To create a contact flow using the contact flow designer**

1. In the navigation pane, choose **Routing, Contact flows**.
2. Choose **Create contact flow**.
3. Type a name and a description for your contact flow.
4. Search for a block using the **Search** bar, or expand the relevant group to locate the block. For more information, see **Contact Block Definitions** (p. 30).
5. Drag and drop blocks onto the canvas. You can add blocks in any order or sequence, as connections between elements aren't required to be strictly linear.
6. Select the block title to access the settings and editing menu.

**To create connections between blocks**

1. Select the originating group.
2. Select the circle for the action to perform.
3. 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.
4. Repeat the steps to create a contact flow that meets your requirements.
5. 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.

**To generate logs for your contact flows**

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 enabling and using contact flow logs, see **Contact Flow Logs** (p. 97).

**To roll back a contact flow**

1. In the contact flow designer, open the contact flow you want to roll back.
2. Use the dropdown 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.

## Create Prompts

Prompts are audio files played in call flows. Only 8 KHz .wav files that are less than 50 MB are supported for prompts. You can upload a pre-recorded .wav file to use for your prompt, or record one in the web application. Prompts and routing policies should be aligned with each other to ensure a smooth call flow for customers.

**To create a prompt**

1. Choose **Routing, Prompts**.
2. On the **Manage voice prompts** screen, choose **+Create new prompt**.
3. You can choose the following actions:
   - **Upload**—Choose the file to upload.
   - **Record**—Choose 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**.

**To manage recorded prompts**

1. Choose **Routing, Prompts**.
2. On the **Manage voice prompts** screen, select the appropriate prompt.
3. You can choose **Play**, **Download**, **Edit**, or **Delete**.
4. Choose **Save**.

## Add Text-to-Speech

Amazon Connect supports text-to-speech, including SSML or plaintext with (or without) dynamic attributes. You can enter text-to-speech prompts in any of the contact flow blocks that support prompt entry, such as **Play prompt** and **Get customer input**. The text-to-speech voice is selected in the **Set voice** contact 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.

Amazon Connect uses Amazon Polly, a service that converts text into lifelike speech using Speech Synthesis Markup Language (SSML). For more information, see **Using SSML** in the Amazon Polly Developer Guide.

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. Amazon Polly provides this level of control using a subset of the SSML markup tags as defined by **Speech Synthesis Markup Language (SSML) Version 1.1, W3C Recommendation**.

**Modify a Prompt using SSML**

When you add a prompt to a contact flow, you can use SSML tags to provide a more personalized experience for your customers. 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.
Create Quick Connects

Calls can be transferred to an agent, a queue, or an external number.

- **External**—Calls are transferred to an external number (such as an on-call pager).
- **Agent**—Calls are transferred to a specific agent as part of a contact flow.
- **Queue**—Calls are transferred to a queue as part of a contact flow.
To add a quick connect

1. Choose **Routing, Quick connects, Add a new destination**.
2. Enter a name for the item, and select a type, destination, contact flow (if applicable), and description.
   
   **Important**
   A description is required when you create a quick connect. An error is returned if you do not add a description.
3. To add more rows, choose **Add a new destination**.
4. Choose **Save**.

To see your quick connects in the contact list in CCP, add them to **Queues**. Agent and queue quick connects only appear when an agent transfers a call.

Add an Amazon Lex Bot

With Amazon Lex, you can build conversational interactions (bots) that feel natural to your customers, giving you access to the same speech recognition and natural language understanding technology that powers Alexa. After you create an Amazon Lex bot, you can add it to your instance and then integrate it into your contact flows. You can add bots from the same Region as your Amazon Connect instance, or from a different Region.

Add an Amazon Lex bot 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. Under **Amazon Lex**, in the **Region** drop-down list, choose the Region in which you created your Amazon Lex bot.
   
   If there are bots associated with your AWS account in the chosen Region, the bots are displayed in the **Bot** drop-down list. If no bots are found in the Region, or when there are no additional bots to add from that Region, the drop-down menu is disabled. A message indicates that there are no bots available to choose in that Region.
5. In the **Bots** drop-down menu, choose your bot, then choose **+ Add Lex bot**.

To create a new bot, choose **Create a new Lex bot** to open the Amazon Lex console. You may need to select a Region where Amazon Lex is available.

To remove a bot from your instance, choose **Remove** next to the bot to remove.

Resume a Contact Flow After Transfer

Use the **Transfer to phone number** block to transfer customers to a phone number outside of your Amazon Connect instance, and then optionally resume the contact flow when the call with the external number ends. This lets you integrate interactions with external or third party organizations into your contact flow. For example, you can use a **Transfer to phone number** block to transfer the caller to a shipping provider to check the status of their delivery, and then return the caller to an agent if they need further assistance. Or, you could send the caller to another department in your organization that is not using Amazon Connect, and return the caller to the Amazon Connect contact flow to speak with an agent.
Using Resume After Transfer in a Contact Flow

You can use the **Transfer to phone number** block to transfer customers to a number outside of your Amazon Connect instance, and then optionally resume the contact flow after the caller disconnects from the external number. You can use the resume after transfer functionality to enable the following scenarios:

- Transfer a caller to a number outside of your instance and end the contact flow. For example, asking the customer for an order number, and then transferring the customer to the delivery company that can provide their shipping status.
- Transfer the customer to a number outside of your instance, and then return the customer to the contact flow to request a survey, or to speak to an agent. For example, when the delivery company could not resolve the issue for the customer.
- 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 prior to the customer being connected.

To resume a contact after a transfer to an external number, add a **Transfer to phone number** block to your contact flow. In the **Transfer to phone number** block, enter the phone number to transfer the call to, and then connect it to the rest of your contact flow. When the block executes, the call is transferred to the external number, and then, optionally, returned to the contact flow when the conversation with the external party ends. The contact then follows the **Success** branch from the block to continue the flow. If the call is not successfully transferred, one of the other branches is followed: **Call failed**, **Timeout**, or **Error**, depending on the reason the caller did not return to the flow.

Transfer to Phone Number Block Settings

The **Transfer to phone number** block includes 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.
  - **Caller ID number**—Specify the caller ID number used for transferred call. You can select a number from your instance, or use an attribute to set the number.
  - **Caller ID name**—Specify the caller ID name used for the transferred call. You can enter a name, or use an attribute to set the name.

In some cases, the caller ID information is provided by the carrier of the party you are calling. The information may not be up-to-date with that carrier, or the number may get passed differently between systems because of hardware or configuration differences. If that is the case, the person
you call may not see the phone number, or may see the name of a previously registered owner of the number, instead of the name you specify in the block.

Initiate an Outbound Call

Use the **Call phone number** 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.

When an outbound call is placed from your contact center, the number used to place the outbound call is the number selected as the **Outbound caller ID number** for the queue with which the outbound whisper flow is associated. The caller ID number displayed to the call recipient is the number used to place the call. In some cases, you may want to display a different number as the caller ID number for your organization. For example, if you have customers in multiple geographic locations, you may want to display a number local to the area where your customers are. Perhaps your organization has multiple lines of business serviced by a single set of agents, and want to display a different number from your instance for each line of business so that customers have the correct number to call back.

When you use a **Call phone number** block in an outbound whisper flow, you can optionally set the caller ID number for outbound calls. You can select any phone number from your instance, or use an attribute to set the number dynamically during the contact flow. The attribute can be a user-defined attribute you create using a **Set contact attributes** block in the contact flow, or an external attribute returned from an AWS Lambda function. When you use an attribute to set the number, the value of the attribute must be a phone number from your instance in E.164 format. If the number is not in E.164 format, the number from the queue associated with the outbound whisper flow is used for the caller ID number. If no number is set for the outbound caller ID number for the queue, the call attempt will fail.

For more information about E.164, see Use E.164 Format for Telephone Numbers (p. 66).

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.

How it Works

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.

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 ACW state.

Manage Calls in a Queue

For calls coming into your contact center, you can define advanced routing decisions to minimize queue wait times, or route calls 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 call 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 in the block to determine which queue to route the call to based on attribute values. For more information about using queue metrics, see Using System Metric Attributes (p. 56).

After determining which queue to transfer the call to, use a Transfer to queue block in a contact flow to transfer the call 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 calls in the queue to the Maximum contacts in queue limit, if one is set for the queue. If no limit is set, the queue is limited to the number of concurrent active calls set in the service limit for the instance.

After the call is placed in a queue, the call remains there until an agent takes the call, or until the call 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.

In the Transfer to queue block, there are two outputs to route calls through: the Success branch or the At capacity branch. When a call is successfully transferred to a queue and follows the Success branch, the call remains associated with the current customer queue flow after being transferred. When the call is not successfully transferred to a queue and follows the At capacity branch because the queue is at capacity, the call remains in the current working queue.

To manage calls 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 Calls Directly to a Specific Agent

With agent queues, you can route calls directly to a specific agent. This can allow you to provide a consistent customer experience for your customers by letting you route calls directly to the agent the customer last interacted with if that agent is available. In each block that supports transferring the contact to a queue, such as the **Transfer to queue** block, there is a **By agent** radio button under **Queue** (or **Queue to check (optional)** or **By queue** depending on the block). When you select **By agent**, a drop-down list that includes all of the users in your instance is displayed. When you select a user name, the contact is transferred to the queue for that user.

Contact flow blocks in which you can specify a queue include: **Set working queue**, **Get queue metrics**, **Check queue status**, **Check staffing**, and **Transfer to queue** when used in a customer queue flow.

**Note**
A queue is created for all users in your Amazon Connect instance, but only users assigned permissions to use the Contact Control Panel (CCP) can use the CCP to receive calls. The Agent or Admin security profiles are the only default security profiles that include permissions to use the CCP. If you route a call to a user that cannot access the CCP, the contact can never be answered.

To route a call 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**.
Under **Select an agent**, enter the user name of the agent, or select the agent's user name from the drop-down list.

*Choose Save.*

*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**.

### Using 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](https://docs.aws.amazon.com/AmazonConnect/latest/APIReference/AmazOnConnect_eventstream.html) (p. 88). 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 example, agent event data, the agent ID is `87654321-4321-4321-4321-123456789012`.

```json
{
    "AWSAccountId": "123456789012",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "Name": "Available",
            "StartTimestamp": "2019-01-02T19:16:11.011Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "IAM",
            "LastName": "IAM",
            "RoutingProfile": {
                "DefaultOutboundQueue": {
                    "Name": "BasicQueue"
                },
                "InboundQueues": [
                    {
                        "Name": "BasicQueue"
                    }
                ],
                "Username": "Basic Routing Profile"
            },
            "Username": "agentUserName"
        },
        "Contacts": []
    }
}
```
Contact Block Definitions

Contact flows are created in the contact flow designer using action blocks, which you arrange by dragging and dropping them onto a grid. The contact flow configuration is grouped into blocks. Each group represents a specific action, and each block has editable conditions related to the group’s action or behavior.

**Note**
When you set User Defined or External values in dynamic attribute fields, ensure that you use only alphanumeric characters (A-Z, 0–9) and periods. No other characters can be used.

### Interact

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play prompt</td>
<td>Plays a stored audio file, or delivers a Text-to-speech message.</td>
<td>Prompts can be an audio file, stored in the prompt library, or text-to-speech, which can optionally be specified in a flow using a contact attribute. If you use text-to-speech, you can use a maximum of 3,000 billed characters (6,000 total characters).</td>
</tr>
<tr>
<td>Get customer input</td>
<td>Branches based on customer intent.</td>
<td>Plays an interruptible audio prompt and branches based on DTMF or Amazon Lex intents. If you use text-to-speech, 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.</td>
</tr>
<tr>
<td>Store customer input</td>
<td>Stores numerical input to contact attribute.</td>
<td>Plays an interruptible audio prompt and stores digits via DTMF as a contact attribute. To enable encryption, contact your system administrator to add a public signing key to the Contact flow security keys settings of your Amazon Connect instance.</td>
</tr>
<tr>
<td>Loop prompts</td>
<td>Loops a sequence of prompts while a customer or agent is on hold or in queue.</td>
<td>When Loop prompts is used in a queue flow, audio playback can be interrupted with a flow at preset times.</td>
</tr>
<tr>
<td>Hold customer or agent</td>
<td>Places a customer or agent on or off hold.</td>
<td>Settings: Agent on hold / customer on call</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer on hold / agent on call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent and customer on call</td>
</tr>
<tr>
<td><strong>Call phone number</strong></td>
<td>Initiates an outbound call from an outbound whisper flow.</td>
<td>Use the Call phone number block to place an outbound call. This block is supported only in outbound whisper flows. You can optionally set the phone number displayed as the caller ID number to a number from your instance, or to a number using an attribute. The number must be in E.164 format.</td>
</tr>
<tr>
<td><strong>Start media streaming</strong></td>
<td>Starts capturing customer audio for a contact.</td>
<td>Captures customer audio during a contact. You must enable Live media streaming to successfully capture customer audio. Media streaming continues until a Stop media streaming block is used or the contact ends. To learn more, see Live Media Streaming in Contact Flows (p. 40).</td>
</tr>
<tr>
<td><strong>Stop media streaming</strong></td>
<td>Stops capturing customer audio after it is started with a Start media streaming block.</td>
<td>Once started, media streaming continues, even when one contact flow transfer to another contact flow. You must use a Stop media streaming block to stop media streaming.</td>
</tr>
</tbody>
</table>

**Set**

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set working queue</strong></td>
<td>Specifies the queue to be used when Transfer to queue is invoked.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To use a Set working queue block to set the queue dynamically, such as with contact attributes, you must specify the ARN for the queue rather than the queue name. To find the ARN for a queue, open the queue in the queue.</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Set call recording behavior</strong> Sets options for call recordings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables or disables call recording for the agent, customer, or both.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Set contact attributes</strong> Stores key-value pairs as contact attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact attributes are accessible by other areas of Amazon Connect, such as the CTRs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Get queue metrics</strong> Retrieves real-time metrics about queues and agents in your contact center and returns them as attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a <strong>Check contact attributes</strong> block to check metric values and define routing logic based on them, such as number of contact in a queue, number of available agents, and oldest contact in a queue. For more information, see Using System Metric Attributes (p. 56).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Change routing priority / age</strong> Alters the priority of the contact in queue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing age alters the time in queue for the contact, which determines its priority in comparison to when other contacts are received.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Queue priority sets the contact to a high priority that can be compared to other contacts that have a priority set (typically between 1 and 1000).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Set hold flow</strong> Links from one contact flow type to another.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the flow to invoke when a customer or agent is put on hold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Set whisper flow</strong> Overrides the default whisper by linking to a whisper flow.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the whisper to be played to customer on an outbound call, or to the customer or agent when the call is joined.</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set callback number</td>
<td>Sets a callback number.</td>
<td>Specifies the number to be used to call the customer back in the CCP, or when Transfer to queue is invoked with the callback option. When specifying a phone number in Amazon Connect, the number must be in E.164 format. Numbers in E.164 format do not include the leading zeroes you would dial for a local or regional call within the same country when dialing the number from a phone. For example, if you usually dial 0400xxxxxx to place a call in Australia, the number in E.164 format includes the country code of 61 and removes the leading zero for the number. The number to use in Amazon Connect is +61400xxxxxx.</td>
</tr>
<tr>
<td>Set voice</td>
<td>Sets the voice.</td>
<td>Sets the voice to interact with the customer, and optionally the voice if using text-to-speech (TTS).</td>
</tr>
<tr>
<td>Set customer queue flow</td>
<td>Set queue flow.</td>
<td>Specifies the flow to invoke when a customer is transferred to a queue.</td>
</tr>
</tbody>
</table>

### Branch

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check queue status</td>
<td>Checks the status of the queue based on specified conditions.</td>
<td>Branches based on the comparison of Time in Queue or Queue capacity. If no match is found, the No Match branch is followed.</td>
</tr>
<tr>
<td>Check staffing</td>
<td>Checks the current working queue, or queue you specify in the block, for whether agents are available, staffed (on call, or after call work status), or online.</td>
<td>Branches based on whether agents are available, staffed (available, on call, and after call work), or online. Important You must set a queue before using a Check staffing block in your contact flow. If a queue is not set, the</td>
</tr>
</tbody>
</table>

Important
You must set a queue before using a Check staffing block in your contact flow. If a queue is not set, the
<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>block always proceeds</td>
<td>block always proceeds through the error</td>
<td>block always proceeds through the error branch. You can use a <strong>Set working queue</strong> block to set the queue. 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.</td>
</tr>
<tr>
<td>Check hours of operation</td>
<td>Checks to see whether the contact is</td>
<td>Branches based on specified hours of operation, either directly or as associated to a queue that is within open hours.</td>
</tr>
<tr>
<td></td>
<td>occurring within or outside of the hours of</td>
<td>Important Queues that are automatically created for each user in your instance do not include an Hours of operation. If you use the block to check the Hours of operation for one of these queues, the check fails and the Error branch is followed.</td>
</tr>
<tr>
<td></td>
<td>operation defined for the queue.</td>
<td></td>
</tr>
<tr>
<td>Check contact attributes</td>
<td>Check the values of contact attributes.</td>
<td>Branches based on a comparison to the value of a contact attribute. Supported comparisons include: <strong>Equals</strong>, <strong>Is Greater Than</strong>, <strong>Is Less Than</strong>, <strong>Starts With</strong>, <strong>Contains</strong>.</td>
</tr>
<tr>
<td>Distribute by percentage</td>
<td>Routes customers randomly based on a</td>
<td>Like flipping a coin, contacts are distributed randomly, which doesn’t guarantee exact percentage splits.</td>
</tr>
<tr>
<td></td>
<td>percentage.</td>
<td></td>
</tr>
<tr>
<td>Loop</td>
<td>Loops through (repeats) the <strong>Looping</strong></td>
<td>After the loops are completed, the <strong>Complete</strong> branch is followed. If you enter 0 for the loop count, the <strong>Complete</strong> branch is followed the first time this block executes.</td>
</tr>
<tr>
<td></td>
<td>branch for the number of loops specified.</td>
<td>An example use of this block is to loop back to a <strong>Get customer input</strong> block to try to enter input, such as an account number, when an initial attempt does not succeed.</td>
</tr>
</tbody>
</table>
## Integrate

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Invoke AWS Lambda function</strong></td>
<td>Makes a call to AWS Lambda, and optionally returns key-value pairs.</td>
<td>The returned key-value pairs can be used to set contact attributes. To use an AWS Lambda function in a contact flow, first add the function to your instance. For more information, see Add an AWS Lambda function to your instance. After you add the function to your instance, you can select the function from the Select a function drop-down list in the block to use it in the contact flow.</td>
</tr>
</tbody>
</table>

## Terminate / Transfer

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disconnect / hang up</strong></td>
<td>Terminates a customer contact.</td>
<td>Disconnects the customer's call.</td>
</tr>
<tr>
<td><strong>Transfer to queue</strong></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 call already in a queue to another queue.</td>
<td>When used in most contact flows, a queue must be specified, using Set working queue, before invoking Transfer to queue except when used in a customer queue flow. Optionally, the contact can be placed in queue to receive a callback, if a Set customer callback number block is used before this block in a flow. When used in a customer queue flow, a Loop prompts block must be used prior to this block in the contact flow.</td>
</tr>
<tr>
<td><strong>Transfer to phone number</strong></td>
<td>Transfers the customer to a phone number external to your instance.</td>
<td>Transfers the contact to the specified phone number. 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 resume the contact flow after the transferred call ends. If the country you want to select is not listed, you can submit a</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>request to add countries you want to transfer calls to using the Amazon Connect service limits increase form.</td>
<td></td>
</tr>
<tr>
<td>Transfer to agent</td>
<td>Transfers the customer to an agent.</td>
<td>Ends the current contact flow and transfers the customer to an agent. If the agent is on a call, the contact is disconnected.</td>
</tr>
<tr>
<td>Transfer to flow</td>
<td>Transfers the customer to another contact flow.</td>
<td>Ends the current contact flow and transfers the customer to a different contact flow. Available in transfer to agent and transfer to queue flows.</td>
</tr>
<tr>
<td>End flow / Resume</td>
<td>Ends the current flow without disconnecting the caller.</td>
<td>This can be used to return to a Loop prompts block when it has been interrupted. When End flow / Resume is invoked, the customer remains connected to the system.</td>
</tr>
</tbody>
</table>

Lambda Functions in Contact Flows

Amazon Connect can interact with your own systems and take different paths in contact flows dynamically. To achieve this, invoke 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. 36)
- Add a Lambda Function (p. 37)
- Invoke the Lambda Function (p. 37)
- Configure Your Lambda Function to Parse the Event (p. 38)
- Verify the Function Response (p. 38)
- Consume the Lambda Function Response (p. 39)

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 (p. 37). 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

After you add a Lambda function to your instance, you can easily use it in your contact flow.

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. For AWS Lambda, select the function to add to your instance from Function. This list contains only the functions in the same Region as the instance. If there are no functions in the list, 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.

Invoke the Lambda Function

Use the following procedure to invoke a Lambda function from your contact flow.

To invoke the function in a contact flow

1. Open or create a contact flow.
2. Insert an Invoke AWS Lambda function block and connect the inputs and outputs.
3. Select the block to edit the configuration.
4. For Lambda function, choose the function. This list contains only the functions that you added to your instance in the previous task.
5. (Optional) Add Function input parameters, which are key-value pairs that are sent to the Lambda function when it is invoked. You can also specify a Timeout value for the function.

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 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-XXXXXXXXXX",
         "CustomerEndpoint": {
            "Address": "+1234567890",
            "Type": "TELEPHONE_NUMBER"
         },
         "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXX",
         "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
         "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/c8c0e68d-2200-4265-82c0-XXXXXXXXXX",
         "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXX",
```
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.

### 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:

```python
def lambda_handler(event, context):
    resultMap = {"Name":"CustomerName","Address":"1234 Main Road","CallerType":"Patient"}
    return resultMap
```

The output returned from the function must be a flat object of key/value pairs, with values that include only alphanumeric, dash, and underscore characters. Nested and complex objects are not supported. The size of the returned data must be less than 32 Kb of UTF-8 data.

The following example shows the JSON output from these Lambda functions:

```json
{
    "Name": "CustomerName",
    "Address": "1234 Main Road",
    "CallerType": "Patient"
}
```

### 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 form 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.
Live Media Streaming in Contact Flows

In Amazon Connect, you can capture the customer audio during an interaction with your contact center by sending the audio to a Kinesis Video Stream. All customer audio is captured in the stream from the customer, starting when the Start media streaming block is invoked in a contact flow. Customer audio is captured for the entire interaction, including when the customer is interacting with an Amazon Lex bot that is used in your contact flow, and when the customer on hold.

The customer audio is stored in Kinesis for the time defined by your retention settings. You can use the customer audio streams to perform analysis on the audio to determine customer sentiment, use the audio for training purposes, or to later review the audio to identify and flag abusive callers. Only customer audio is sent to Kinesis Video Streams. Audio sent to Kinesis uses a sampling rate of 8 Khz.

When you enable media streaming in Amazon Connect, one Kinesis Video stream is used per call. The default Kinesis service limit for the Number of Video Streams is 100 streams per AWS account. To make sure that there are enough streams available for all calls in your contact center, set the limit for the Number of Video Streams to a value greater than the number of the maximum concurrent active calls for your instance. If you have more than one instance for your AWS account, increase the Number of Video Streams limit to a number greater than the concurrent active calls for all of your instances combined.

Enable Live Media Streaming

Live media streaming (customer audio streams) is not enabled by default. You can enable customer audio streams from the settings page for your instance.

To enable live media streaming

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. 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 Stream 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.

Example Contact Flow for Testing Live Media Streaming

In a contact flow, add a Start media streaming block in the flow at the point where you want to enable customer audio streaming. Connect the Success branch to the rest of your flow. When you want to stop customer media streaming, add a Stop media streaming block to the flow. 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 demonstrates using 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.

### Live Media Streaming Contact Attributes

The attributes, displayed when you select **Media streams** for the **Type** in a contact flow block that supports attributes include the following:

**Customer audio stream ARN**

The ARN of the Kinesis Video stream that includes the customer data to reference.

Customer audio start timestamp

The time at which the customer audio stream started.

**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.

**JSONPath format:** $.MediaStreams.Customer.Audio.StopPosition

For more information about Amazon Kinesis Video Streams fragments, see [Fragment](#) in the *Amazon Kinesis Video Streams Developer Guide*.

### How to Access Kinesis Video Stream Data

Use the steps and code samples in this section to interact with the customer audio data sent to Kinesis Video Streams.

First, download the [Kinesis Video parser library](#).

Next, 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 KVS Parser library that gets media from the specified Kinesis Video Stream with the specified fragment number.
- **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.

Then, use Audacity (https://www.audacityteam.org/), or other audio tool, to import the .raw audio file, which is a 16-bit signed PCM Mono format.

### Code Samples to Access Kinesis Video Stream Data

**LMSDemo.java**

```java
package com.amazonaws.kinesisvideo.parser.demo;

import com.amazonaws.auth.AWSSessionCredentials;
import com.amazonaws.auth.AWSSessionCredentialsProvider;
import com.amazonaws.kinesisvideo.parser.examples.LMSExample;
import com.amazonaws.regions.Regions;
```
import java.io.FileOutputStream;
import java.io.IOException;

public class LMSDemo {
    public static void main(String args[]) throws InterruptedException, IOException {
        LMSExample example = new LMSExample(Regions.US_WEST_2, "<<StreamName>>", "<<FragmentNumber>>", new AWSSessionCredentialsProvider() {
            @Override
            public AWSSessionCredentials getCredentials() {
                return new AWSSessionCredentials() {
                    @Override
                    public String getSessionToken() {
                        return "<<AWSSessionToken>>";
                    }
                    @Override
                    public String getAWSAccessKeyId() {
                        return "<<AWSAccessKey>>";
                    }
                    @Override
                    public String getAWSSecretKey() {
                        return "<<AWSSecretKey>>";
                    }
                };
            }
            @Override
            public void refresh() {
            }
        }, 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.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 outputStream;
    private final String fragmentNumber;

    public LMSExample(Regions region,
                       String streamName,
                       String fragmentNumber,
                       AWSCredentialsProvider credentialsProvider,
                       OutputStream outputStream) throws IOException {
        super(region, credentialsProvider, streamName);
        this.streamOps = new StreamOps(region, streamName, credentialsProvider);
        this.executorService = Executors.newFixedThreadPool(2);
        this.outputStream = outputStream;
        this.fragmentNumber = fragmentNumber;
    }

    public void execute () throws InterruptedException, IOException {
        getMediaProcessingArguments = GetMediaProcessingArguments.create(outputStream);
        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");
            }
        }
    }

    private static class LogVisitor extends MkvElementVisitor {
        private final FragmentMetadataVisitor fragmentMetadataVisitor;

        private LogVisitor(FragmentMetadataVisitor fragmentMetadataVisitor) {
            this.fragmentMetadataVisitor = fragmentMetadataVisitor;
        }

        public long getFragmentCount() {
            return fragmentCount;
        }
    }
}

private long fragmentCount = 0;

@Override
public void visit(MkvStartMasterElement startMasterElement) throws MkvElementVisitException {
    if (MkvTypeInfos.EBML.equals(startMasterElement.getElementMetaData().getTypeInfo())) {
        fragmentCount++;
        System.out.println("Start of segment");
    }
}

@Override
public void visit(MkvEndMasterElement endMasterElement) throws MkvElementVisitException {
    if (MkvTypeInfos.SEGMENT.equals(endMasterElement.getElementMetaData().getTypeInfo())) {
        System.out.println("End of segment");
    }
}

@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 outPutStream) 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(outPutStream));

        return new GetMediaProcessingArguments(frameVisitor);
    }

    @Override
    public void close() throws IOException {
    }
}
LMSFrameProcessor.java

```java
package com.amazonaws.kinesisvideo.parser.utilities;
import com.amazonaws.kinesisvideo.parser.mkv.Frame;
import java.io.IOException;
import java.io.OutputStream;
import java.nio.ByteBuffer;
public class LMSFrameProcessor implements FrameVisitor.FrameProcessor {
    private OutputStream outputStream;

    protected LMSFrameProcessor(OutputStream outputStream) {
        this.outputStream = outputStream;
    }

    public static LMSFrameProcessor create(OutputStream outputStream) {
        return new LMSFrameProcessor(outputStream);
    }

    @Override
    public void process(Frame frame, MkvTrackMetadata trackMetadata) {
        saveToOutputStream(frame);
    }

    private void saveToOutputStream(final Frame frame) {
        ByteBuffer frameBuffer = frame.getFrameData();
        try {
            byte[] frameBytes = new byte[frameBuffer.remaining()];
            frameBuffer.get(frameBytes);
            outputStream.write(frameBytes);
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

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 with a human agent, 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.
Using Contact Attributes

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.

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

- **System**—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**—A subset of system attributes related to agents in your contact center.
- **Queue metrics**—System metric attributes returned when you use a `Get queue metrics` block in your contact flow.
- **User-defined**—Attributes that are created when a contact flow executes 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**—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**—External attribute for the slot name of an Amazon Lex bot.
- **Lex attributes**—Session attributes from an Amazon Lex bot interaction.

**Using 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 call flow based on comparing an attribute to a value. You then route the call 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.

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.

**Capture Customer Input and Store it as an Attribute**

You can use an attribute to request a callback number from a customer, store the value of the attribute, and then reference the attribute in a `Set callback number` block to set the number to dial the customer. You could also use a `Store customer input` block to capture any numeric input from a customer, such as an account or order number.
To create an attribute from customer input with a Store customer input block

1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing contact flow, or create a new one.
3. Add a Store customer input block.
4. Edit the block, and select Text to speech (Ad hoc).
5. In the Enter text box, type a message that is said to customers when they call, such as “Please enter your phone number.”
6. In the Customer input section, select Phone number, and then choose the format. Local format is for a number in the same country as the region in which you created your Amazon Connect instance. International format/Enforce E.164 is for numbers to a country other than the country in which you created your instance.
Store customer input

Stores numerical input to contact attribute.

Prompt

- Select from the prompt library
- Text to speech (Ad hoc)

Learn more about Amazon Connect's TTS capabilities

- Enter text

Please enter your phone number.

- Enter dynamically

Interpret as

Text

Prompt

- Custom

Phone number

- Local format

<table>
<thead>
<tr>
<th>Country code</th>
<th>Delay between entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1</td>
<td>5</td>
</tr>
</tbody>
</table>

in seconds
7. Add a Set callback number block to your contact flow, and connect it to the Get customer input block.

8. Under Use attributes, for Type, choose System. For Attribute, choose Stored customer input. The callback number is set to the number the customer entered when asked to enter their phone number.

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.

**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.

**Using Attributes in the Contact Control Panel**

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.

Referencing 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 calls in a queue, then route the call to the queue if the active calls are fewer than 5. You can also route the call to another different queue if the number of active calls 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 call to a queue that has fewer than 5 active contacts in it.

Using a Check contact attributes block to route a call 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 call, 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 call 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.

Using 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. 60).

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 call 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, you can 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 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.

- **Dialled 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 the customer used to call your contact center, but 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. It 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. Currently only VOICE is supported.

- **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.

- **Lex intent**—The name of the intent as defined in your Amazon Lex bot.

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>$.CustomerEndpoint.Address</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Dialed number</td>
<td>The number the customer dialed to call your contact center.</td>
<td>System</td>
<td>$.SystemEndpoint.Address</td>
</tr>
<tr>
<td>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>$.TextToSpeechVoiceId</td>
</tr>
<tr>
<td>Contact id</td>
<td>The unique identifier of the contact.</td>
<td>System</td>
<td>$.ContactId</td>
</tr>
<tr>
<td>Initial contact id</td>
<td>The unique identifier for the 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. Currently, only VOICE is supported in Amazon Connect.</td>
<td>System</td>
<td>$.Channel</td>
</tr>
<tr>
<td>Instance ARN</td>
<td>The ARN for your Amazon Connect instance.</td>
<td>System</td>
<td>$.InstanceARN</td>
</tr>
<tr>
<td>Initiation method</td>
<td>How the contact was initiated. Valid values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, and API.</td>
<td>System</td>
<td>$.InitiationMethod</td>
</tr>
<tr>
<td>System Endpoint Type</td>
<td>The type of the system endpoint. Valid value is TELEPHONE_NUMBER.</td>
<td>System</td>
<td>$.SystemEndpoint.Type</td>
</tr>
</tbody>
</table>
### Contact Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<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>

### 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>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>
</tbody>
</table>
### Contact Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<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>

**External Contact Attributes**

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>Metrics queue size</td>
<td>The number of contacts currently in the queue.</td>
<td>System</td>
<td>$.Metrics.Queue.Size</td>
</tr>
<tr>
<td>Oldest contact in queue</td>
<td>For the contact that has been in the queue the longest, the length of time that the contact has been in the queue, in seconds.</td>
<td>System</td>
<td>$.Metrics.Queue.OldestContactAge</td>
</tr>
<tr>
<td>Agents online</td>
<td>The number of agents currently online, which means logged in and</td>
<td>System</td>
<td>$.Metrics.Agents.Online.Count</td>
</tr>
</tbody>
</table>
## Contact Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<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>$.Metrics.Agents.Staffed.Count</td>
</tr>
<tr>
<td>Agents in After contact work</td>
<td>The number of agents currently in the ACW state.</td>
<td>System</td>
<td>$.Metrics.Agents.AfterContactWork.Count</td>
</tr>
<tr>
<td>Agents busy</td>
<td>The number of agents currently active on a contact.</td>
<td>System</td>
<td>$.Metrics.Agents.Busy.Count</td>
</tr>
<tr>
<td>Agents missed count</td>
<td>The number of agents in the Missed state, which is the state an agent enters after a missed call.</td>
<td>System</td>
<td>$.Metrics.Agents.Missed.Count</td>
</tr>
</tbody>
</table>

## Media Streams Attributes

The following table lists the attributes you can use to identify the location in the live media stream where the customer audio starts and stops.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer audio stream ARN</td>
<td>The ARN of the Kinesis Video stream used for Live media streaming that includes the customer data to reference.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StreamARN</td>
</tr>
<tr>
<td>Customer audio stop timestamp</td>
<td>When the customer audio stream stopped the Kinesis video</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StopTimestamp</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>JSONPath Reference</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Customer 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.StartPosition</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.

**Contact Flow Import/Export**

You can export contact flows from and import contact flows into your Amazon Connect instance. You can use exported contact flows to create backup copies and manage version control of your contact flows. This lets you easily restore a previous version in case you encounter an error with a published contact flow. You can easily copy contact flows from one Amazon Connect instance to another, for example from a test environment to a production environment, or from one Region to another as you expand your customer service organization.

**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.
Because Amazon Connect contact flows are not tied to a specific instance or account, exported flows could also be imported into instances created by other customers, allowing Amazon Connect partners to create custom contact flow solutions that can be used by Amazon Connect customers.

When you export a contact flow, the most recently saved version of the flow you currently have open in the Contact Flow editor is exported as a UTF-8 encoded JSON document. Each block of your contact flow is included in the JSON document as a separate section. To import a contact flow, either one that you previously exported, or that was exported from a different Amazon Connect instance, you just select the JSON file and import it. The imported flow replaces the contact flow currently open in the editor. The imported contact flow is not added to your Amazon Connect instance until you save it after importing.

### Resolving 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.

### Exporting Contact Flows

When you export a contact flow, the JSON document created for the flow 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 folder that contains only exported contact flows.

**Important**

When you attempt to import or export a large or complex contact flow, the export may fail if the contact flow contains a large amount of blocks and resources. It may also fail if the file size for the exported contact flow exceeds 1 MB in size. An notification message is displayed when this occurs.

**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:
   - To replace an existing contact flow with the one you are importing, open the contact flow to replace.
   - Create a new contact flow of the same type as the one you are importing.
4. Choose **Save, Import flow**.
5. Select the file to import, and choose **Import**.
6. Review and update any resolved or unresolved references as necessary.
7. To save the imported flow, choose **Save**. To publish, choose **Save and Publish**.
Amazon Connect Contact Control Panel

Agents use the Amazon Connect Contact Control Panel (CCP) to communicate with contacts. They can use the CCP with a softphone or a desk phone.

As the admin, you manage the phone numbers at the instance level, not in the CCP. For more information, see Phone Numbers for Your Contact Centers (p. 10).

Amazon Connect CCP Concepts

Amazon Connect provides a number of management and configuration options for your contact center. The terminology and concepts that are central to your understanding and use of Amazon Connect are described below.

agent

Users who handle contacts using Amazon Connect.

softphone

A browser-based telephony service that is not linked to a handset. It can be used remotely, provided that the agent is logged in to Amazon Connect.

desk phone/handset

A physical telephone requiring an agent to be in its proximity in order to make or receive calls.

status

Metrics are gathered based on changes in agent status (available, offline, and so on).

after contact work

A state where the agent is no longer on a call but has related work to complete before being able to accept or make other calls.

leave

Leave a multi-party call without disconnecting the other parties or hanging up the call.

Access the Amazon Connect CCP

As the admin, you can access the CCP by clicking on the phone icon in the upper right corner of Amazon Connect.

Before agents can access to the CCP and handle contacts, however, there are a few things you need to do:

- Add them as users to the instance. For more information, see Manage Users (p. 8).
• Configure their permissions. 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 Amazon Connect Security Profiles (p. 80).
• Give them their user name, password, and a link to the CCP so they can log in. The default link is https://name of your instance.awsapps.com/connect/ccp#/

We recommend telling agents to bookmark the URL to the CCP so they can access it easily.

Grant Microphone Access

If agents experience problems with their microphone, they may need to grant microphone access in their browser.

For Google Chrome steps, see Use your camera and microphone in Chrome.

For Mozilla Firefox steps, see Firefox Page Info window.

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.

Use E.164 Format for Telephone Numbers

Amazon Connect requires phone numbers in E.164 format. E.164 is an international public telecommunication numbering plan defined by the International Telecommunication Union (ITU). Using phone numbers in E.164 format ensures that numbers are interpreted consistently when placing calls between countries, and when phone numbers are passed between software applications and telephony services.

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

E.164 defines a general format for international telephone numbers. Numbers are limited to a maximum of 15 digits, excluding the international call prefix. The presentation of a number is usually prefixed with the plus sign (+), indicating that the number includes the country calling code. When dialing, the number must typically be prefixed with the appropriate international call prefix (in place of the plus sign), which is a trunk code to reach an international circuit from within the country of call origination. 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 being originated.

To express a US phone number to E.164 format, add the ‘+’ prefix and the country code (1) in front of the number. 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 xxxxx in the UK would be formatted as +44 20 718 xxxxx.

Set up Softphones and Desk Phones

Before agents can use the CCP, check the following configurations:
- **Headset connectivity**—Check the settings in Device Management to ensure that your computer recognizes the headset and allows proper headset connectivity.
- **Set up headset**—You may need to adjust your browser settings to ensure correct peripheral selection.
- **Desktop notifications**—Ensure that the browser is not in incognito mode so that desktop notifications can be displayed.
- **Microphone**—Ensure that the microphone settings are always enabled.
- **Dialing**—In **Settings**, you can configure the softphone to dial a DID desk phone if required. When you choose a desk phone, enter the DID number to which calls go.

## Softphone CCP IP Address Ranges

If your agents use a softphone for Amazon Connect, you must allow traffic in both directions for the ports and addresses listed below, for the region in which you created your instance.

The IP addresses used by Amazon Connect for each region are listed, along with the addresses for all AWS services, in the [https://ip-ranges.amazonaws.com/ip-ranges.json](https://ip-ranges.amazonaws.com/ip-ranges.json) file under the service name AMZON_CONNECT. For agents to use the CCP, you also need to allow access for the softphone signaling endpoints, which are hosted in Amazon EC2. For more information about IP address ranges in AWS, see [AWS IP Address Ranges](https://aws.amazon.com/ip-address-ranges/).

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available [ip-ranges.json](https://aws.amazon.com/ip-address-ranges/) 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Transport Layer</th>
<th>IP Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>AWS EC2 and CLOUDFRONT ranges in <a href="https://ip-ranges.amazonaws.com/ip-ranges.json">https://ip-ranges.amazonaws.com/ip-ranges.json</a></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>AWS EC2 and CLOUDFRONT ranges in <a href="https://ip-ranges.amazonaws.com/ip-ranges.json">https://ip-ranges.amazonaws.com/ip-ranges.json</a></td>
</tr>
<tr>
<td>TURN</td>
<td>3478</td>
<td>UDP</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>

## Status Settings

The status settings are used for reporting purposes to ensure that system issues are resolved quickly and to manage resources.

The following settings are available:

- **Available**—Indicates that an agent is available to take calls.
- **Offline**—Logs agents out and removes them from the pool of available agents.
Application Integration

All domains that embed the CCP for a particular instance must be explicitly whitelisted for cross-domain access to the instance. For example, to integrate with Salesforce, you must whitelist your Salesforce Visualforce domain.

**To whitelist 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**.

Accept and Transfer Calls

When agents use the Contact Control Panel (CCP), they can perform the following actions on a softphone. When they opt for a desk phone, they have the same controls as softphone. The only difference is that there is no **Accept** button on a desk phone.

**Accept Incoming Calls**

- To accept an incoming call, choose **Accept call**.
- To edit settings, choose **Settings**.
- To end a call, choose **End call**.
- To put a call on hold, choose **Hold**.

When a call is connected, a new set of options become available in the CCP.

**Transfer Calls**

After an agent picks up a call, they can transfer the call by choosing the **Transfer** button and then choosing one of the available contacts. To define this list of available contacts, you set up quick connects. The quick connects are displayed in the list of contacts when an agent tries to transfer an active call.

Agents can also manually enter a phone number to transfer calls to by choosing **Dial number** after answering the call. The agent can enter a phone number using the keypad, and then choose **Transfer** to transfer the call. If agents regularly transfer calls to a specific external phone number, you can create an **External** contact flow and use that phone number for the destination.

**To set up call transfers and quick connects**

1. Create and publish a contact flow for the type of transfer to enable.
   - To enable transfers to another agent, create a Transfer to agent contact flow.
   - To enable transfers to a queue, create a Transfer to queue contact flow.
   - External transfers do not require a specific type of contact flow.

   **Note**
   You must publish your contact flows to make them active in your contact center.
2. 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.

For more information about quick connects, see Create Quick Connects (p. 23).

3. Add the quick connect that you created to any queue used in a contact flow for which to enable call transfer, such as the queue used in the contact flow for incoming calls. The queue must be in the routing profile assigned to the agent who should be able to transfer calls.

To transfer calls to an agent or queue

1. After accepting a call in the CCP, choose Transfer.
2. Select the contact to whom to transfer the call, and then choose Dial.

   The call is placed on hold during the transfer.
3. After the call is answered by an agent, or sent to a queue, choose Leave call to disconnect from the call.
4. To use conference, swap, or hold:

   • To begin a conference call, choose Join to perform a soft transfer. To drop out of the call, choose Leave.
   • Choose Swap to switch between talking to a customer and the person to whom you’re transferring the call.
   • Choose Hold all to put all parties on hold.

Some settings that are configured in Amazon Connect include setting agents to go into the After call work state after they are done with their call. Agents can also be configured to accept a call automatically, without having to choose Accept.

Listen in to Calls

Managers can listen in on active calls as agents interact with customers. To set this up, you need to add the Set call recording block to your contact flow, assign managers the appropriate permissions, and then show them how to listen in.

Important

The listen-in feature works only when call recording is enabled on a contact flow. For instructions on adding the Set call recording block to your contact flow, see Work with Recordings (p. 70).

Assign Permissions to Listen to Calls

These permissions enable managers to listen to active calls and access recordings of past calls.

To assign the manager permissions to listen in to 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. Also assign the manager to the Agent security profile so they can access the control contact panel.
4. 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. Expand Contact Control Panel, then choose Access Contact Control Panel and Make outbound calls.
5. Choose Save.

Listen in to Calls

To listen in on active agent calls
1. 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.
2. Open the CCP by choosing the phone icon in the top-right corner of your screen. You'll need the CCP open to connect to the call.
3. To choose the agent call you want to listen in to, in Amazon Connect choose Metrics and quality, Real-time metrics, Agents.
4. Next to the names of agents on a call, you'll see a headset icon. Choose the icon to start listening to the call.
   When you're listening to call, the status in your CCP changes to Monitoring.
5. To stop listening to the call, in the CCP choose End call.
   When the agent ends the call, monitoring stops automatically.

Work with Recordings

Managers can listen to and download recordings of agent calls. To set this up, you need to add the Set call recording behavior block to your contact flows, grant managers the appropriate permissions, and show them how to access the recordings in Amazon Connect.

To set up call recording 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 listen in on.
3. Before the call is connected to an agent, add a Set call recording behavior block to the contact flow. In the block, choose Agent and Customer, and then choose Save.
   Important
   Make sure that the block has connections to the block before and after it in the contact flow.
4. To enable manager listen-in and recording for outbound calls, the contact flow in which you add Set call recording behavior must be in the flow selected as the outbound contact flow for the queue used for outbound calls.
5. Choose **Save and Publish** to publish the updated contact flow. Choose **Save and Publish** again to confirm that you want to overwrite the published version.

**To assign the manager permissions to listen in to recordings of 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. Also assign the manager to the **Agent** security profile so they can access the control contact panel.
4. Choose **Save**.

**Listen to or Download Recordings**

**To listen to or download recordings of agents talking to customers**

1. 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.
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. Calls that were recorded will have icons in the Recording column. Click to listen to a recording, download, or delete it. If you choose to download the file, it will be saved automatically to your Downloads folder.

**Call Back Customers**

You can create contact flows that provide the ability for customers to leave their phone number and get a call back. For an example contact flow, see the Sample queued callback template.

When a customer leaves their number it's put in a queue and then routed to the next available agent.

**To see the number of customers waiting for call backs**

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, which counts all customers who are in a queue for an agent.

To only see a count of the customers waiting for a call back, you need to create a queue that only takes callback contacts. To learn how to do this, see **Amazon Connect Queues (p. 17)**.

**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 and a AWS Serverless application deployed to your AWS environment.

With those components, customers can build a deep integration between the Amazon Connect contact center platform and Salesforce, the leading customer relationship management (CRM) platform. The collection of pre-build utilities enables a rapid integration between these two platforms. The AWS
Serverless application package contains a set of common Lambda functions to be used by Amazon Connect to interact with Salesforce.

**About the Adapter**

The key benefits of the adapter include:

- Agent state synchronization between Salesforce Omni and Amazon Connect
- Provide valuable information to the agent through configurable view of call attributes
- Utilize the Amazon Connect Call Campaign Object for automated outbound dialling
- Automatically create phone call tasks and relate it to the right Salesforce object
- Embed Amazon Connect Call Recordings in the Salesforce record
- Automatically clean-up open tabs to improve agent efficiency
- Easily enable lookup, create and update operations for different Salesforce objects, like Contacts and Cases, within Amazon Connect contact flows.
- Support Salesforce Sales and Service Console in Classic and Lightning.

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.

The next step is to whitelist your Salesforce Visualforce domain within Amazon Connect. This allows cross-domain access to your Amazon Connect instance.

This page provides a quick setup guide. Please review the [Amazon Connect CTI Adapter v3 for Salesforce installation guide](#) for a more detailed walk-through and setup of the full CTI Adapter capabilities. We also have a trailhead available at [https://sfdc.co/Amazon-Connect](https://sfdc.co/Amazon-Connect). Note, it's still in process of being updated to support latest CTI Adapter features.

**Prerequisites**

Before the Amazon Connect CTI package can be installed, the following prerequisites need to be fulfilled:

- Salesforce Classic, Salesforce Console, or Lightning Experience
- Create an Amazon Connect instance ([https://aws.amazon.com/connect/](https://aws.amazon.com/connect/)).
- Salesforce Omni-Channel must be activated in the Salesforce org. For more information, see Enable Omni-Channel.

**Browser Compatibility**

Amazon Connect requires WebRTC to enable soft-phone voice media stream and Websockets to enable soft-phone signalling. Consequently, users are required to use the latest version of either Google Chrome or Mozilla Firefox. For more details, please see the Amazon Connect FAQ page.

**To integrate with Salesforce**

1. In your Salesforce sandbox, install the following managed package: Amazon Connect CTI Adapter.
2. Edit one of appropriate call center configuration (Amazon Connect CCP Adapter Classic, Console, or Lightning).
   - For Amazon Connect CCP URL, type the CCP URL for your instance (for example, [https://instance.awsapps.com/connect/ccp](https://instance.awsapps.com/connect/ccp)).
• For Phone Number Formatting, Country, specify the appropriate 2-digit ISO country code.
• To provide Salesforce users with access to the Amazon Connect CCP, on the Setup Call Centers page, choose Manage Call Center Users. Add the Salesforce users to enable for using these call features. Be sure to add your own Salesforce user account if you plan to these features.

3. Whitelist your Salesforce Visualforce domain URL using the directions in Application Integration (p. 68). To verify the URL, open the Visualforce page in setup. This URL usually has the following format:

   https://amazonconnect.your-instance-name.visual.force.com

4. Log in to your Amazon Connect instance.

5. Launch Salesforce. You should see the integrated CCP in the side panel (Salesforce Classic) or the phone toolbar (Salesforce Classic and Lightning Experience).

Troubleshooting Common Issues

If you encounter errors with your configuration, check the following common issues:

• Confirm that Salesforce is not blocking your iFrame. For more information, see Enable Clickjack Protection for Visualforce Pages Even When Headers Are Disabled.
• Confirm that the Amazon Connect user is assigned only the Agent security profile.
• Confirm that your Salesforce Call Center Phone Number Formatting is configured with the following parameters:

   {"OPF":"0","NPF":"2 digit dialing code","Country":"2 digit country code","NF":"International Plaintext","TNF":"(555) 123-4567"}

• Confirm that the Salesforce user can access the call center. To check a user's status, choose Manage Call Center Users.
• Under Softphone Layout, Screen Pop, confirm that Single-matching record is set to Pop detail page and Multiple-matching record is set to Pop to search page.
• If you are using Salesforce Lightning Experience and do not see a phone toolbar icon, confirm that you have enabled console navigation. To enable console navigation, in the Salesforce Setup Console, choose App Manager, Service Console (Lightning), Edit. On the Edit page, choose App Options, App Navigation, Console Navigation.
Identity Management in Amazon Connect

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

You can choose from one of the following supported 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. 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 directory. 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 for Identity Management in Amazon Connect (p. 75).

Use an Existing Directory for Identity Management

If you are already using a in 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 Service Pricing Overview.

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

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

Configure SAML for Identity Management in 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
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?

Steps for configuring SAML include:
- Overview of Using SAML with Amazon Connect (p. 75)
- Enabling SAML-based Authentication for Amazon Connect (p. 76)
- Select SAML 2.0-based Authentication During Instance Creation (p. 77)
- Enable SAML Federation Between Your Identity Provider and AWS (p. 77)
- Use a Destination in Your Relay State URL (p. 79)
- Add users to Your Amazon Connect Instance (p. 79)
- SAML User Logging in and Session Duration (p. 80)

Overview of Using SAML with Amazon Connect

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

1. The user browses to an internal portal that includes a link to log in to Amazon Connect. The link is defined in the identity provider.
2. The federation service requests authentication from the organization’s identity store.
3. The identity store authenticates the user and returns the authentication response to the federation service.
4. When authentication is successful, the federation service posts the SAML assertion to the user’s browser.
5. The user’s browser posts the SAML assertion to the AWS sign in SAML endpoint (https://signin.aws.amazon.com/saml). AWS sign in receives the SAML request, processes the request, authenticates the user, and forwards the authentication token to Amazon Connect.
6. Using the authentication token from AWS, Amazon Connect authorizes the user and opens Amazon Connect in their browser.

**Enabling SAML-based Authentication for Amazon Connect**

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

1. Create an Amazon Connect instance and select SAML 2.0-based authentication for identity management.
2. Enable SAML federation between your identity provider and AWS.
3. Add Amazon Connect users to your Amazon Connect instance. Log in to your instance using the administrator account created when you created your instance. Go to the User Management page and add users. The user names must exactly match the user name in your network directory and your identity provider.
4. Configure your identity provider for the SAML assertions, authentication response, and relay state. Users log in to your identity provider. When successful, they are redirected to your Amazon Connect instance. The IAM role is used to federate with AWS, which allows access to Amazon Connect.
Select SAML 2.0-based Authentication During Instance Creation

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

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

Enable SAML Federation Between Your Identity Provider and AWS

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

The process to create an identity provider for AWS is the same for Amazon Connect. For step 7 in the flow diagram, 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. The IAM role determines which permissions the users that log in through your identity provider have in AWS. In this case, the permissions are for accessing Amazon Connect. You can control the permissions to features of Amazon Connect by using security profiles in Amazon Connect. For more information, see Creating a Role for SAML 2.0 Federation (Console).

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

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

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

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

```json
{
   "Version": "2012-10-17",
   "Statement": [
   {
       "Sid": "Statement1",
       "Effect": "Allow",
       "Action": "connect:GetFederationToken",
       "Resource": [
       ]
   ]
}```
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:

   ```text
   https://region-id.console.aws.amazon.com/connect/federate/instance-id
   ```
Replace the \textit{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 \textit{instance-id} with the instance ID for your instance.

\textbf{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 \textbf{Instance ARN} displayed on the \textbf{Overview} page. For example, the instance ID in the following Instance ARN is \textit{178c75e4-b3de-4839-a6aa-e321ab3f3770}.

\texttt{arn:aws:connect:us-east-1:450725743157:instance/178c75e4-b3de-4839-a6aa-e321ab3f3770}

\section*{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 \texttt{URL encoding} for the destination value used in the URL:

\begin{verbatim}
https://us-east-1.console.aws.amazon.com/connect/federate/instance-id?
destination=%2Fconnect%2Fccp
\end{verbatim}

\section*{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 \textbf{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 \textbf{Access denied} message is displayed.

\begin{center}
\textbf{Access denied}
\end{center}

\begin{quote}
Your user account has not been added to Amazon Connect. Please ask your admin to add you, and then try again.
\end{quote}

\section*{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 \textbf{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 \textbf{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.

![Session expired](image)

Amazon Connect Security Profiles

Security profiles consist of permissions that determine which Amazon Connect users can view, update, or create which Amazon Connect resources or perform specific tasks. Assigning a security profile to a user grants that user the permissions you added to the security profile. For example, you can grant users read/write access to routing profiles.

Security profiles are organized into the following permission groups:

- **Routing**—Grant access to routing profiles, quick connects, hours of operation, and queues.
- **Numbers and flows**—Grant access to prompts, contact flows, and phone numbers.
- **Users and permissions**—Grant access to users, agent hierarchies, security profiles, and agent status.
- **Contact Control Panel (CCP)**—Grant access to the CCP and to make outbound calls.
- **Metrics and Quality**—Grant access to metrics, contact search, contact attributes, login/logout reports, manager listen in, call recordings, and saved reports.
- **Historical Changes**—Grant access to view historical changes.

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.
Considerations

- When you grant permission to edit users, you also grant permission to reset user passwords, including that of the administrator.
- When you grant permission to create or edit users, you also grant permission to assign users a security profile that grants them full access to the contact center.
- 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 do a search of calls, 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.

Default Security Profiles

We provide 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 are the default security profiles:

- **Admin**—Grants administrators permission to perform all actions.
- **Agent**—Grants agents permission to access the CCP.
- **CallCenterManager**—Grants managers permission to perform actions related to user management, metrics, and routing.
- **QualityAnalyst**—Grants analysts permission to perform actions related to metrics.

Create a Security Profile

Creating a security profile enables you to grant your users only the permissions that they need.

**To create a security profile**

1. Log in to your contact center using your access URL (https://domain.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 update security profiles**

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
Assign a Security Profile to a User

To assign a security profile to 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 one or more users and choose Edit.
4. 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.
5. Choose Save.

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 GetBucketAcl for the S3 bucket specified for call recordings.
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.
- **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.

**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.
Monitoring Amazon Connect

You can use the following features to monitor your Amazon Connect contact centers.

**Login/logout reports**

You can capture information about the login and logout times for each agent session. For more information, see Login/Logout Reports (p. 84).

**Agent event streams**

You can use agent event streams to capture near real-time information about agent activity in your contact center. For more information, see Amazon Connect Agent Event Streams (p. 88).

**Contact flow logs**

You can use contact flow logs to capture detailed information about the events in your contact flows as customer interact with them. For more information, see Contact Flow Logs (p. 97).

**CloudWatch metrics**

You can use Amazon CloudWatch to retrieve statistics about data points for your contact centers as an ordered set of time-series data, known as metrics. You can use these metrics to verify that your contact center is performing as expected. For more information, see CloudWatch Metrics for Your Amazon Connect Instance (p. 100).

---

**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.

You can view the report in the Amazon Connect interface, download the report, or share it with other users. You can set a schedule for the days of the week to generate the report, and you can filter the report on agent, agent hierarchy, or routing profile to include only records for a specific set of agents in the report.

**Considerations**

- Only users that have the Login/Logout report permission see Login/Logout report listed under Metrics and quality. For more information, see Login/Logout Report Permissions (p. 85).
- Closing the browser does not log the user out. The report does not show that a user has logged out until the user clicks the logout button. The user is shown as logged in from the previous login until the next time the user clicks the logout button.
- A Login/Logout report can contain up to 10,000 rows. When you generate a Login/Logout report that includes more than 10,000 rows, the report fails to complete. If you generate a report and view it on the Login/Logout report page, you receive an error if you attempt to display a page of the report beyond row 10,000. If you schedule a Login/Logout report that contains more than 10,000 rows, the report fails, no report output is 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. For more information, see Generate a Login/Logout Report (p. 85).

Login/Logout Report Permissions

By default, only users assigned the Admin security profile for an Amazon Connect instance are granted permission to generate and view the Login/Logout reports. To allow other users to view a shared report, or to schedule or generate the report, your Amazon Connect admin must assign the Login/Logout report permission to a role assigned to that user. To enable other users in other roles to generate or view the reports, add the permission to the security role assigned to those users.

In Amazon Connect, permissions are assigned to security profiles. The permission a user has is determined by the security role assigned to the user account. Only users that are assigned a security profile that has been granted the View permission for Login/Logout reports can view published reports. If you share a link with a specific user, that user can only view the report if his or her account has explicit permission to do so using their security profile. If you do not want to grant the permission to one of the security profiles included with Amazon Connect, you can create a custom security profile and assign permissions to that role. Users can be assigned more than one security profile, so you could make a profile that grants permissions only to Login/Logout reports and then assign specified users to that profile.

To assign Login/Logout report permissions

1. Open the Amazon Connect dashboard.
3. Select the security profile for which to modify permissions.
4. Choose Metrics and Quality.
5. In the Login/Logout report row, select All to grant all permissions, or View to only grant permissions to view shared reports.
6. Choose Save.

Generate a Login/Logout Report

When you generate a Login/Logout report, it 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.

When you create your report, you can filter the results in the report by Agent, Agent hierarchy, Routing profile, or None (show all agents). For the time frame, you can select Today (since 12 am), Last 24 hours, Yesterday, Last 2 days, Last 3 days, or Custom time range.

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.
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 LoginLogout 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.

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: .../Reports/my-prefix/report-name-YYYY-MM-DD…
8. Choose Create.

After you schedule a report, you can change or delete the schedule for it at any time.

To edit or delete the schedule for a report

1. Follow the steps in the preceding section to open the Schedule report page.
2. To edit the schedule, choose Edit, update the Recurrence and Delivery Options as desired, and then choose Save.
3. To delete the schedule for the report, choose Delete, and then choose Delete again on the confirmation dialog.

Delete a Saved Login/Logout Report

Too many reports in your report library? If you no longer want to use a saved report, you can delete it. When you delete a report, you are only deleting the settings for the report, not any reports that have already been generated using those settings. No CSV files created from a scheduled report are removed from your S3 bucket.

To delete a saved Login/Logout report

1. Open your Amazon Connect dashboard.
2. Choose **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 agent login, agent logout, agent answers a call, and agent status change.

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.

### Enabling 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 call recordings or scheduled reports. 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 call recording or scheduled reports encryption 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**.

**Use Agent Event Streams to Determine Agent ACW Time**

You can use agent event stream data to determine the amount of time an agent spent in ACW. Though there is no event in the event stream for the agent entering ACW status, you can use the other agent event data to calculate the time.
In agent event streams, you can determine the time at which an agent entered ACW status by viewing the `StateStartTimeStamp` for the event for a contact entering the ENDED state in the event stream.

For example, in the following example agent event stream output, the agent enters ACW at 

```
```
Agent ACW state ends when the agent enters another state, such as when the agent chooses a status in the CCP. To determine the time at which an agent left ACW status, you can view the EventTimestamp for the EventType "STATE_CHANGE" in the stream output. Note that a STATE_CHANGE event also occurs when the agent’s configuration is changed, such as the routing profile assigned to the agent. To
confirm that you are using the correct EventTimeStamp associated with the agent leaving ACW status, use the EventTimeStamp for the event where the associated CurrentAgentSnapshot has no contacts listed, and the state for the contact listed in the PreviousAgentSnapshot equals ENDED.

For example, in the following example agent event stream file, the agent left ACW at "EventTimestamp": "2018-10-25T18:55:32.032Z".

```json
{
  "AWSAccountId": "012345678901",
  "CurrentAgentSnapshot": {
    "AgentStatus": {
      "Name": "Available",
      "StartTimestamp": "2018-10-25T18:43:59.059Z"
    },
    "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": []
  },
  "EventId": "477f2c4f-cd1a-4785-b1a8-97023dc1229d",
  "EventType": "STATE_CHANGE",
  "PreviousAgentSnapshot": {
    "AgentStatus": {
      "Name": "Available",
      "StartTimestamp": "2018-10-25T18:43:59.059Z"
    },
    "Configuration": {
      "AgentHierarchyGroups": null,
      "FirstName": "(Removed)",
      "LastName": "(Removed)",
      "RoutingProfile": {
```
To calculate the amount of time an agent spent in ACW, subtract the "StateStartTimestamp": "2018-10-25T18:55:27.027Z" from the "EventTimestamp": "2018-10-25T18:55:32.032Z". In this example, the value is 5.005 seconds.

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:
  - Agent configuration, such as profile or the assigned hierarchy group.
  - Agent state in the contact control panel, such as Available.
  - Agent conversation state, such as on hold.
• HEART_BEAT—This event is published every 120 seconds if there are no other events published during that interval.

Event Objects
• AgentEvent (p. 93)
• AgentSnapshot (p. 94)
• Configuration (p. 94)
• Contact Object (p. 95)
• HierarchyGroup Object (p. 96)
• AgentHierarchyGroups Object (p. 96)
• Queue Object (p. 97)
• RoutingProfile Object (p. 97)

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:ssZ)

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 2017-10-10.

Type: String

AgentSnapshot

The AgentSnapshot object includes the following properties:

AgentStatus

Agent status data, including:
• AgentARN—the ARN for the agent.
• Name—the name of the status, such as Available or Offline.
• StartTimestamp—The time stamp 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 Flow Logs

Amazon Connect contact flow logs provide you with real-time details about events in your contact flows as customers interact with them. You can use contact flow logs to help debug your contact flows as you are creating them. After you publish your contact flows, you can view the logs to gain insight into what happens during complex contact flows, and quickly identify errors that your customers encounter when
they connect to your contact center. If needed, you can always roll back to a previous version of a contact flow.

Contact flow logs are stored in Amazon CloudWatch, in the same region as your Amazon Connect instance. 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. As a contact center manager, you can aggregate data from contact flow logs to analyze performance of contact flows to optimize the experience you provide for your customers. For more information about CloudWatch Logs, see the Amazon CloudWatch Logs User Guide.

Enabling Contact Flow Logs

To start generating contact flow logs, enable contact flow logs for your Amazon Connect instance. After you enable logs for your instance, logs are generated only for contact flows that include a `Set logging behavior` block with logging set to enabled. You can control which flows, or parts of flows, logs are generated for by including multiple `Set logging behavior` blocks and setting logging to enabled or disabled as desired. 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 having logging settings persist between flows, you should include a `Set logging behavior` block in the flow with logging enabled or disabled as desired for that specific flow.

When you create a new Amazon Connect instance, you can enable Contact flow logs when you configure Data Storage settings. If you already have an Amazon Connect instance, you can enable or disable Contact flow logs for your instance in the Amazon Connect console under Contact flow settings. You are not charged for generating contact flow logs, but are charged for using CloudWatch for generating and storing the logs. Free tier customers are charged only for usage that exceeds service limits. For details about Amazon CloudWatch pricing, see Amazon CloudWatch Pricing.

To enable contact flow logs for your Amazon Connect instance

1. Open the Amazon Connect console.
2. Choose the instance alias for the instance for which to enable contact flow logs.
3. Choose Contact flows.
4. Select Enable Contact flow logs and choose Apply.

After you enable contact flow logs for your instance, you can enable logging for a flow by adding a `Set logging behavior` block.

To enable or disable contact flow logs for a contact flow

1. Add a `Set logging behavior` block and connect it to another block in the flow.
2. Open the settings for the block, and under Logging behavior do one of the following:
   - Select Enable to turn on logging for the flow.
   - Select Disable to turn off logging for the flow.
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.

Data Captured 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 control which data is captured in contact flow logs by including a **Set logging behavior** block in your contact flow. 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 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-1264-42e3-9a73-62cbb3c9a45",
"ContactFlowModuleType": "SetQueue",
"Events": {
  "Queue": [
    "arn:aws:connect:us-east-2:670047220557:instance/d-92673ef044/queue/f0300e43-9547-477c-b8ba-0bb7a72f7fa1"
  ]
}
```

**Tracking Customers Between Contact Flows**

In many cases, customer contacts interact with multiple contact flows in your call 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.

**Analyzing Contact Flow Logs with Amazon Kinesis**

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.
CloudWatch Metrics for Your Amazon Connect Instance

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 number of voice calls that exceeded the concurrent active calls limit for the instance. This is a count of the number of calls that exceeded the limit, not the number of concurrent calls in excess of the limit.

Unit: Count

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 limits.

Unit: Count

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

CallsPerInterval

The number of voice calls, both inbound and outbound, received or placed per second in the instance.

Unit: Count

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.

Unit: Count

ConcurrentCallsPercentage

The percentage of the concurrent active voice calls service limit used in the instance. This is calculated by ConcurrentCalls/ConfiguredConcurrentCallsLimit * 100.
Unit: Percent

**ContactFlowErrors**

The number of times the error branch for a contact flow was executed.

Unit: Count

**ContactFlowFatalErrors**

The number of times a contact flow failed to execute due to a system error.

Unit: Count

**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

**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.

Unit: Seconds

**MisconfiguredPhoneNumbers**

The number of calls that failed because the phone number is not associated with a contact flow.

Unit: Count

**PublicSigningKeyUsage**

The number of times a contact flow security key (public signing key) was used to encrypt customer input in a contact flow.

Unit: Count

**QueueCapacityExceededError**

The number of calls that were rejected because the queue was full.

Unit: Count

**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

**ThrottledCalls**

The number of voice calls that were rejected because the rate of calls per second exceeded the maximum supported limit. To increase the supported rate of calls, request an increase in the service limit for concurrent active calls per instance.

Unit: Count

**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.
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

Filters metric data by contact flow. Includes the following metrics:

- CallRecordingUploadError
- ContactFlowErrors
- ContactFlowFatalErrors
- MisconfiguredPhoneNumbers
- PublicSigningKeyUsage

Instance Metrics Dimension

Filters meta data by instance. Includes the following metrics:

- CallsBreachingConcurrencyQuota
- CallsPerInteval
- ConcurrentCalls
- ConcurrentCallsPercentage
- MissedCalls
- ThrottledCalls

Instance ID, Participant, Stream Type, Type of Connection

Filters metric data by connection. Includes the following metrics:

- ToInstancePacketLossRate

Queue Metrics Dimension

Filters metric data by queue. Includes the following metrics:

- CallBackNotDialableNumber
- LongestQueueWaitTime
- QueueCapacityExceededError
- QueueSize
Amazon Connect Metrics and Contact Trace Records

In Amazon Connect, data about contacts, such as the amount of time a contact spends in each state (customer on hold, customer in queue, agent interaction time) are captured in contact trace records (CTR). 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 metrics in the report are calculated using the data captured in the CTRs.

Not all metrics are derived from CTR data.

Within Amazon Connect, you can generate a number of real-time and historical metric reports to monitor efficiency and utilization, agent performance, and other information about your contact center. CTRs are available within your instance for 24 months from the time at which the associated contact was initiated. You can also choose to stream CTRs to Amazon Kinesis so that you can manage retention and perform advanced analysis on the data for your contact center.

To get detailed information on the activity of agents in your contact center, you can use Amazon Connect Agent Event Streams (p. 88).

Contents
- Real-time Metrics Reports (p. 103)
- Historical Metrics Reports (p. 108)
- Contact Trace Records Data Model (p. 115)

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.

Data in real-time metrics reports is refreshed as follows:

- The **Real-time metrics** page refreshes every 15 seconds.
- 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.

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 Amazon Connect Security Profiles (p. 80).

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. 105).
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 download your saved real-time metrics reports, choose QualityAnalyst, Saved reports, and then choose the Real-time metrics tab.

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.

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.
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.

**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.

**Active**
- Indicates whether the agent is currently active on a contact. The value is 1 (true) or 0 (false).

**ACW**
- Count of agents with a status of AfterCallWork.

**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.

**AHT**
- Average time, from start to finish, that a contact was connected with an agent (average handled time). This is calculated by averaging the amount of time between the contact being answered by an agent and the contact ending.

**API contacts handled**
- Count of contacts that were initiated by an API operation, such as StartOutboundVoiceContact, and handled by an agent.

**Availability**
- Indicates whether the agent is currently in the Available status. The value is 1 (true) or 0 (false).

**Available**
- Count of agents with a status of 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 an agent spent in the AfterCallWork status during the specified time range.

**Avg hold time**
- Average time, in seconds, that a contact in the queue was on hold.
**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:

\[
\text{Avg hold time} + \text{Avg interaction time}
\]

**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.

**Callback contacts handled**

Count of contacts handled by an agent that were queued callbacks.

**Consult**

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 most recent contact the agent handled.

**Duration**

Amount of time that the agent has been in the current status.

**Error**

Count of agents with a status of 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.

**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.
Missed

Count of contacts routed to an agent but not answered by the agent, including contacts abandoned by the customer, during the specified time range. A contact can be counted as missed multiple times, once for each time it is routed to an agent but not answered.

NPT

(Non-Productive Time) Count of agents in a custom status (any status other than Available, Error, or Offline.) Agents can handle contacts while in a custom status.

Occupancy

Percentage of time the agent was active on contacts during the specified time range.

Oldest

Length of time in the queue for the contact that has been in the queue the longest.

On call

Count of agents currently on a contact.

Online

Count of agents with a status other than Offline.

Queue

The name of the queue associated with the most recent contact the agent handled.

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.

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 logged in and with a status of Available, On call, or ACW.

Status

The current status of the agent. Possible values include Available and AfterCallWork.

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. 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

- Grouping Options (p. 108)
- Filters (p. 109)
- Create a Historical Metrics Report (p. 109)
- Schedule a Historical Metrics Report (p. 110)
- Update a Historical Metrics Report (p. 111)
- Download a Historical Metrics Report (p. 111)
- Historical Metrics Definitions (p. 111)

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 do not specify any queues, all queues are included.
- **Routing profile**—Includes data only for the agents assigned to the specified routing profiles. If you do not 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 do not 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 do not specify a phone number, data for all contacts associated with all phone numbers is included.

Create a Historical Metrics Report

You can create historical metrics reports to view data for past activity in your contact center.

**Requirement**

- You must have permission to access metric data. The following security profiles include this permission: `CallCenterManager` and `QualityAnalyst`. For more information, see Amazon Connect Security Profiles (p. 80).

**Limits**

- You can get data only for active queues. A queue is inactive if there are no contacts in the queue and no agents available.
- The user interface shows up to 100 queues. If you have more than 100 active queues, you can add a filter to scope the report to the queues of interest.
- A report can contain up to 80K cells (`columns * rows`).

**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
To customize your report, choose the gear icon.

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, chose 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 group by the first grouping option and then by the subsequent grouping options. For more information, see Grouping Options (p. 108).

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. 109).

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. 111).

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**.

**Schedule a Historical Metrics Report**

Scheduling a report makes the report accessible by any other users for your contact center that have permissions to view saved reports. Any user with permission to edit saved reports can also modify your scheduled reports. 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.

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.

**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 the pattern for the recurrence (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.

## 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 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.

When the report is exported to your Amazon S3 bucket, the file name for the exported file includes the date and UTC time at which 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.

**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.

## Historical Metrics Definitions

The following metrics are available to include in historical metrics reports in Amazon Connect.

**After contact work time**

Total time that an agent spent in the After Contact Work (ACW) status after handling a contact. Agents enter the ACW status after a contact ends and leave it when they select a different agent status.

**Agent answer rate**

Percentage of contacts routed to an agent that were answered.

**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.
Agent idle time

Total time that an agent spent in a productive status without handling contacts. The productive statuses include Available and Error.

Agent interaction and hold time

Sum of the Agent interaction time and Customer hold time metrics.

Agent interaction time

Total time that agents spent interacting with customers on a contact. This does not include hold time or after contact work.

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.

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 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.

This metric appears as Contacts missed in scheduled reports and exported CSV files.

Agent on contact time

Total time that an agent spent on a contact, including hold time and after contact work. This does not include time spent on a contact while in a custom status.

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.

API contacts handled

Count of contacts that were initiated using an Amazon Connect API operation, such as StartOutboundVoiceContact, and handled by an agent.

Average after contact work time

Average time that an agent spent in the After Contact Work (ACW) status. This is calculated by averaging AfterContactWorkDuration (from the CTR) for all contacts included in the report, based on the selected filters.

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 and CustomerHoldDuration.

Average agent interaction time

Average time that agents interacted with customers during contacts.

Average customer hold time

Average time that customers spent on hold while connected to an agent. This is calculated by averaging CustomerHoldDuration (from the CTR).
**Average handle time**

Average time that agents spent on contacts, including hold time and after contact work.

**Average outbound after contact work time**

Average time that agents spent in the After Contact Work (ACW) status after an outbound contact.

**Average outbound agent interaction time**

Average time that agents spent interacting with a customer during an outbound contact.

**Average queue abandon time**

Average time that contacts waited in the queue before being abandoned. This is calculated by averaging the difference between EnqueueTimestamp and DequeueTimestamp (from the CTR) for abandoned contacts. An contact is considered abandoned if it was removed from a queue but not answered by an agent or queued for callback.

**Average queue answer time**

Average time that contacts waited in the queue before being answered by an agent. This is the average of Duration (from the CTR).

**Callback contacts**

Count of contacts that were initiated from a queued callback.

**Callback contacts handled**

Count of contacts that were initiated from a queued callback and handled by an agent.

**Contact flow time**

Total time a contact spent in a contact flow.

Outbound contacts do not start in a contact flow, so outbound contacts are not included.

**Contact handle time**

Total time that an agent spent on contacts, including hold time and After contact work time. This includes any time spent on contacts while in a custom status.

**Contacts abandoned**

Count of contacts disconnected by the customer while in the queue. Contacts queued for callback are not counted as abandoned.

**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.

**Contacts agent hung up first**

Count of contacts disconnected where the agent disconnected before the customer.

**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. The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

**Contacts consulted**

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.

**Contacts handled**

Count of contacts handled by an agent, including both incoming and outgoing contacts.
Contacts handled incoming

Count of incoming contacts that were handled by an agent, including inbound contacts, transferred contacts, and scheduled callbacks.

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.

Contacts hold agent disconnect

Count of contacts that were disconnected by the agent while the customer was on hold.

Contacts hold customer disconnect

Count of contacts that were disconnected by the customer while the customer was on hold.

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.

Contacts incoming

Count of incoming contacts, including inbound contacts and transferred contacts.

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.

This metric appears as Agent non-response on the Historical metrics page in the user interface.

Contacts put on hold

Count of contacts put on hold by an agent one or more times.

Contacts queued

Count of contacts placed in the queue.

Contacts transferred in

Count of contacts transferred to the queue by an agent using the CCP.

Contacts transferred in from queue

Count of contacts transferred to the queue from another in a Transfer to queue contact flow.

Contacts transferred out

Count of contacts transferred from the queue after being answered by an agent.

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.

Contacts transferred out from queue

Count of contacts transferred from the queue to another queue in a Transfer to queue contact flow.

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.
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.

Error status time

Total time that an agent spent in the Error status. This metric can't be grouped or filtered by queue.

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.

Non-Productive Time

Total time that agents spent in a custom status (any status other than Available, Error, or Offline), including any time they spent handling contacts while in a custom status. This metric can't be grouped or filtered by queue.

Occupancy

Percentage of time that agents were active on contacts. This percentage is calculated as follows:

\[(\text{Agent Handle Time} / (\text{Agent Handle Time} + \text{Agent Idle Time})) * 100\]

Online time

Total time that an agent spent in a status other than Offline. This includes any time spent in a custom status. This metric can't be grouped or filtered by queue.

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:

\[(\text{Contacts removed from queue in X seconds} / \text{Contacts queued}) * 100\]

Contact Trace Records Data Model

This document describes the data model for Amazon Connect contact trace records. Contact trace records capture the events associated with a contact in your contact center. Real-time and historical metrics are based on the data captured in contact trace records.

Agent

Information about the agent that handled the 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.
Agent

**Type:** Integer

**Min value:** 0

**AfterContactWorkEndTimestamp**

The date and time the agent left the After Contact Work status.

**Type:** String (yyyy-mm-ddThh:mm:ssZ)

**AfterContactWorkStartTimestamp**

The date and time the agent entered the After Contact Work status.

**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.

**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.

**Type:** AgentHierarchyGroups (p. 117)

**LongestHoldDuration**

The longest time, in whole seconds, that the customer was put on hold by the agent.

**Type:** Integer

**Min value:** 0

**NumberOfHolds**

The number of times the customer was put on hold while connected to the agent.

**Type:** Integer

**Min value:** 0

**RoutingProfile**

The routing profile of the agent.

**Type:** RoutingProfile (p. 121)

**Username**

The username of 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. 117)

Level2

The group at level two of the agent hierarchy.

Type: AgentHierarchyGroup (p. 117)

Level3

The group at level three of the agent hierarchy.

Type: AgentHierarchyGroup (p. 117)

Level4

The group at level four of the agent hierarchy.

Type: AgentHierarchyGroup (p. 117)

Level5

The group at level five of the agent hierarchy.

Type: AgentHierarchyGroup (p. 117)

ContactTraceRecord

Information about a contact.
Agent
If this contact successfully connected to an agent, this is information about the agent.
Type: Agent (p. 115)

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
The contact channel.
Valid values: VOICE

ConnectedToSystemTimestamp
The date and time the customer endpoint connected to Amazon Connect. 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. 120)

DisconnectTimestamp
The date and time that the customer endpoint disconnected from Amazon Connect.
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 | OUTBOUND | TRANSFER | CALLBACK | API | QUEUE_TRANSFER

InitiationTimestamp

The date and time this contact was initiated. 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.

Type: String (yyyy-mm-ddThh:mm:ssZ)

MediaStreams

The media streams.

Type: Array of MediaStream (p. 120)

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. 120)

Recording

If recording was enabled, this is information about the recording.

Type: RecordingInfo (p. 121)
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. 120)

TransferCompletedTimestamp

If this contact was transferred out of Amazon Connect, the date and time the transfer endpoint was connected.

Type: String (yyyy-mm-ddThh:mm:ssZ)

TransferredToEndpoint

If this contact was transferred out of Amazon Connect, the transfer endpoint.

Type: Endpoint (p. 120)

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 on the contact.

Type

Type: MediaStreamType

Valid value: AUDIO

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. Either the customer disconnected or the contact was connected to an agent.

Type: String (yyyy-mm-ddThh:mm:ssZ)

Duration

The difference in time, in whole seconds, between EnqueueTimestamp and DequeueTimestamp.

Type: Integer
Min value: 0

EnqueueTimestamp

The date and time the contact was added to the queue.

Type: String (yyyy-mm-ddThh:mm:ssZ)

Name

The name of the queue.

Type: String
Length: 1-256

RecordingInfo

Information about a recording.

DeletionReason

If the recording was deleted, this is the reason entered for the deletion.

Type: String

Location

The location, in Amazon S3, for the recording.

Type: String
Length: 0-256

Status

The recording status.

Valid values: AVAILABLE | DELETED

Type

The recording type.

Valid values: AUDIO

RoutingProfile

Information about a routing profile.
**ARN**

The Amazon Resource Name of the routing profile.

Type: ARN

**Name**

The name of the routing profile.

Type: String

Length: 1-100
Amazon Connect Troubleshooting and Best Practices

Use this guide to identify best practices for using Amazon Connect. Also, to troubleshoot information when something isn't working quite how it should.

Contents
- Best Practices for Using the Contact Control Panel (p. 123)
- Troubleshooting Issues with the CCP (p. 128)
- Validation Testing (p. 131)

Best Practices for Using the Contact Control Panel

This guide provides information about the CCP soft phone, including best practices and troubleshooting. For workstations unable to meet soft phone connectivity requirements or experiencing soft phone issues, the CCP also features the ability to redirect to an external device.

Contents
- Agent Workstation Requirements (p. 123)
- Network Ports and Protocols (p. 124)
- Using Amazon Connect in a VDI Environment (p. 126)
- CCP Connectivity (p. 127)

Agent Workstation Requirements

Agent 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 calls, can impact the quality of experience.

Under-powered workstations can make it difficult for agents to access the tools and resources they need to service callers. 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. For the best agent and customer audio experience, a USB headset is recommended. Alternatively, you can redirect the call to an external number, in E.164 format, using an agent's existing telephony.

The following values are the minimum system requirements for the workstations using the CCP only. Additional memory, bandwidth, and CPU should be scoped 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

Monitoring Workstations

There are many factors that can affect CCP functionality at the workstation level. Access to various levels of logging information is essential in determining steps towards remediation. Adding additional logging
and monitoring to workstations that are experiencing resource contention may further reduce available resources and invalidate test results. We recommended that your workstation meet the minimum requirements outlined in the Agent Workstation Requirements (p. 123) section of this guide, leaving 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)
  - Disk / drive
  - RAM / memory
  - Network throughput and performance
- Monitor all of the preceding for your VDI desktop environment, including RTT/packet monitoring between the agent workstation and the VDI environment.

### Network Ports and Protocols

The CCP soft phone requires three connections to AWS resources. You must open the address and port to these resources with the appropriate protocol for the Region in which you created your Amazon Connect instance to allow bi-directional communication for full functionality of the CCP. The CCP needs access to the IP ranges for Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudFront, and Amazon Connect, which are listed in the https://ip-ranges.amazonaws.com/ip-ranges.json file under Amazon EC2 (EC2), CloudFront (CLOUDFRONT), and Amazon Connect (AMAZON_CONNECT) respectively. The address ranges in the file are updated as new resources are added. This means that you need to monitor the included ranges and update your environment accordingly to ensure that agents can use the CCP successfully. 30 days after new IP ranges are added to this file, they start being used by Amazon Connect.

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Connect</td>
<td>3478</td>
<td>UDP in/out</td>
<td>Used for media endpoints within the Region, and for call audio for the softphone client.</td>
</tr>
<tr>
<td>Amazon Connect</td>
<td>443</td>
<td>TCP in/out</td>
<td>CCP signaling endpoint</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>443</td>
<td>TCP in/out</td>
<td></td>
</tr>
<tr>
<td>CloudFront</td>
<td>443</td>
<td>TCP in/out</td>
<td>Used for hosting web content associated with your instance. Endpoints are determined by the</td>
</tr>
</tbody>
</table>
Alternatively, for Amazon EC2 endpoints, you can allow access for the following URL and port to allow all Amazon EC2 endpoints rather than all of the IP Address ranges listed in the AWS ipranges.json file:

rtc.connect-telecom.{region}.amazonaws.com:443

Replace {region} with the Region in which you created your Amazon Connect instance, such as us-east-1. In certain proxy applications, web socket handling may impact functionality when using this address. You should perform testing to validate before deploying to a production environment.

For CloudFront, you can use the following URL with port 443 to allow traffic for all CloudFront endpoints. Do this instead of including all ranges listed in the AWS ipranges.json file:

https://myInstanceName.awsapps.com

Replace myInstanceName with the name of the instance for which to allow traffic. In certain proxy applications, web socket handling may impact functionality when using this address, so you should perform testing to validate before deploying to a production environment.

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, requires the endpoints in the Region closest to where your agents are located. If you have agents in multiple Regions, you need to allow traffic for the endpoints in each Region where agents are using the Amazon Connect CCP. For example, if your instance is US East, and you have an agent physically located in another country, you would need to open the ports for CloudFront using the IP address ranges for the Region where the agent is located.
- Update the ranges for which traffic is allowed within the 30 days after the ranges are updated in the AWS ipranges.json file. If you don’t, you may experience intermittent connectivity issues when using the CCP with a softphone when traffic is routed to the new ranges, but not allowed to connect to your agents using the CCP.
- 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, callers, 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 call state until they or a supervisor changes their state back to available.

### Using AWS Direct Connect

AWS Direct Connect can help solve for latency and poor call quality between your edge router and AWS resources. It also allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN. This allows for a durable, consistent connection rather than relying on your ISP to dynamically route requests to AWS resources. Keep in mind that this does not solve issues with the private LAN/WAN traversal to your edge router.

### 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.

Troubleshooting Issues with the CCP

Troubleshooting CCP issues requires support from your network operations, system administrator, and 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

- Common CCP Issues (p. 128)
- Useful Troubleshooting Tools and Information (p. 129)
- Gathering Helpful Information using the Streams API (p. 130)
- Analyzing the Data (p. 131)

Common 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 whitelist entries, not allowing browser microphone access, or not answering your external device. Be sure that you have whitelisted all IPs covered in the Network Ports and Protocols (p. 124) 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 whitelisted. For more information, see the Network Ports and Protocols (p. 124) 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 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 can also be related to browser microphone permissions or headset issues. For more information, see the Monitoring Workstations (p. 123) 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 Monitoring Workstations (p. 123) 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 Monitoring Workstations (p. 123) 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 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 CTR—Provide when you contact AWS support.
• **Agent desktop performance/process logs**—can help rule out local resource/network contention.

• **Contact Control Panel 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 whitelist access**—to verify that IP/port ranges are whitelisted as described in **Network Ports and Protocols** (p. 124).

• **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.

**Example Agent Issue Report Disposition**

The following example disposition keys are listed by symptom, scenario, and severity.

**Symptom**

- **S**—Softphone error
- **M**—Missed calls
- **L**—Latency causes poor quality
- **P**—Starts off OK, gets progressively worse over time
- **D**—Disconnected calls
- **W**—One way audio; for example, the agent can hear the customer, but the customer cannot hear the agent
- **V**—Volume too quiet or too loud
- **C**—Choppy/cuts in and out intermittently

**Scenario**

- **O**—Outbound call
- **I**—Inbound call
- **T**—Three-way call

**Severity**

- **1**—Small impact, but can use the CCP effectively
- **2**—Medium impact, communication is difficult, but can still service calls
- **3**—Large impact, cannot use the CCP to take calls
Examples

- 5:45PM agentName LT2 (latency on a three-way call with medium impact).
- 6:05PM agentName DO3 (disconnected three-way call with large impact).
- 6:34PM agentName MI3 (missed inbound call with large impact).

Analyzing the Data

The following guidelines can assist you in analyzing the data to identify issues in your environment.

- Use the 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.

- \([\text{overall\_latency}]\) is the total latency experienced between caller and agent. This latency can be calculated as \([\text{overall\_latency}] = [\text{agent\_latency}] + [\text{pstn\_latency}]\).
- \([\text{pstn\_latency}]\) is the latency between Amazon Connect endpoint and the caller. This latency can be calculated as \([\text{pstn\_latency}] = [\text{overall\_latency}] - [\text{agent\_connection\_latency}]\). This latency can be improved by using a different Amazon Connect Region location or avoiding external and circular transfers to geographically distant endpoint locations.
- \([\text{agent\_latency}]\) is the latency between Amazon Connect endpoint and the agent. This latency can be calculated as \([\text{agent\_latency}] = [\text{overall\_latency}] - [\text{recording\_latency}]\). This latency can be improved by using AWS Direct Connect for agents on-premises, avoiding the use of VPN connections, improving private WAN/LAN performance/durability, or using an Amazon Connect Region location closer to...
your agents. Depending on your use case, selecting a different Region selection may also increase [pstn_latency].

- [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

- 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 \[\text{overall\_latency}\].
12. Optionally, to calculate \[\text{agent\_latency}\], 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 \[\text{recording\_latency}\]. \[\text{agent\_latency}\] = \[\text{overall\_latency}\] - \[\text{recording\_latency}\]. 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 \[\text{overall\_latency}\] 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. 131).
Amazon Connect Service Limits

The following table provides the default limits for new Amazon Connect instances. Because the limits have been adjusted over time, the limits in place for your account may be different than the limits described here. There may even be differences between the instances created for your account. For example, if you created an instance when the default limit for concurrent active calls was 10, the limit is 10 concurrent active calls. If you create a new instance today, the limit for the instance is 100 concurrent active calls. For API request limits, see Amazon Connect API Throttling Limits (p. 135).

To start, you can create five instances per AWS account in each of AWS Regions where Amazon Connect is available. If you need more instances, or a change to a service limit, request a change using the Amazon Connect service limits increase form. You must be signed in to your AWS account to access the form.

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. 11).

There is also a service limit for the countries to which you can place outbound calls from your 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 limits over time. You can submit a service limit increase request to allow calling to additional countries, or to limit the countries that you can call from your instance.

Note
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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Default limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Connect instances per account</td>
<td>5</td>
</tr>
<tr>
<td>Users per instance</td>
<td>500</td>
</tr>
<tr>
<td>Phone numbers per instance</td>
<td>10</td>
</tr>
<tr>
<td>Queues per instance</td>
<td>50</td>
</tr>
<tr>
<td>Queues per routing profile</td>
<td>50</td>
</tr>
<tr>
<td>Routing profiles per instance</td>
<td>100</td>
</tr>
<tr>
<td>Hours of operation per instance</td>
<td>100</td>
</tr>
<tr>
<td>Quick connects per instance</td>
<td>100</td>
</tr>
<tr>
<td>Prompts per instance</td>
<td>500</td>
</tr>
<tr>
<td>Agent status per instance</td>
<td>50</td>
</tr>
<tr>
<td>Security profiles per instance</td>
<td>100</td>
</tr>
<tr>
<td>Contact flows per instance</td>
<td>100</td>
</tr>
</tbody>
</table>
### Amazon Connect API Throttling Limits

When you use the Amazon Connect 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.

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Default limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent hierarchy groups per instance</td>
<td>50</td>
</tr>
<tr>
<td>Reports per instance</td>
<td>500</td>
</tr>
<tr>
<td>Scheduled reports per instance</td>
<td>50</td>
</tr>
<tr>
<td>Concurrent active calls per instance</td>
<td>100</td>
</tr>
<tr>
<td>Phone Number Porting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can port your US phone numbers from your current carrier to Amazon Connect. For information about how to port your phone number, see Port Your Current Phone Number (p. 11).</td>
</tr>
<tr>
<td>Country code whitelisting for Outbound Calls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can place calls to the following dialing codes when you create a new instance:</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 limit increase request.
Release Notes

To help you keep track of the ongoing updates and improvements to Amazon Connect, we publish monthly release notices that describe the changes we've released in the previous month.

Monthly Updates
- June 2019 Update (p. 136)
- February 2019 Updates (p. 136)
- January 2019 Updates (p. 137)
- December 2018 Updates (p. 138)
- November 2018 Updates (p. 138)
- October 2018 Updates (p. 139)
- September 2018 Updates (p. 139)
- August 2018 Updates (p. 140)
- July 2018 Updates (p. 140)
- June 2018 Updates (p. 141)
- April and May 2018 Updates (p. 142)

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.

February 2019 Updates

The following updates were released in February 2019:

Updates by category
- Contact Routing (p. 136)
- Contact Flows (p. 137)
- Metrics and Reporting (p. 137)
- Contact Control Panel (CCP) (p. 137)

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. 137)
• Contact Flows (p. 137)
• Metrics and Reporting (p. 137)

## 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**.
December 2018 Updates

The following updates were released in December 2018:

**Updates by category**
- Metrics and Reporting (p. 138)
- Contact Control Panel (CCP) (p. 138)

**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. 138)
- Contact Flows (p. 138)
- Metrics and Reporting (p. 139)

**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. 139)
- Metrics and Reporting (p. 139)
- API (p. 139)

General

- Resolved an issue that sometimes resulted in stuck media sessions.

Metrics and Reporting

- Resolved an issue that sometimes resulted in agent names not being displayed correctly in historical reports.
- Resolved an issue that sometimes resulted in the data related to agent Auxiliary states being incorrectly overwritten.

API

- Resolved an issue where the GetCurrentMetrics operation returned the metric OLDEST_CONTACT_AGE was returned in milliseconds instead of seconds.

September 2018 Updates

The following updates were released in September 2018:

Updates by category
- General (p. 139)
- API (p. 140)

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. 140)
  • Contact Routing (p. 140)
  • Metrics and Reporting (p. 140)

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. 141)
  • General (p. 141)
  • Metrics and Reporting (p. 141)
  • Contact Flows (p. 141)
New Features

- Initiate an Outbound Call (p. 26)
- Add an Amazon Lex Bot (p. 24)
- User Management APIs
- Manage Calls in a Queue (p. 27)

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. 141)
- Telephony and Voice (p. 141)
- Contact Flows (p. 142)
- Metrics and Reporting (p. 142)
- Contact Control Panel (CCP) (p. 142)

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 Initiate an Outbound Call (p. 26).
• Released contact attributes for system metrics, including a new Get metrics block in contact flows. For more information, see Using System Metric Attributes (p. 56).

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. 142)
• Telephony and Voice (p. 143)
• Contact Flows (p. 143)
• Metrics and Reporting (p. 143)
• Contact Control Panel (CCP) (p. 143)

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.
## Document History

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added information about the updated <strong>Transfer to phone number</strong> block</td>
<td>You can use the updated <strong>Transfer to phone number</strong> 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. 24).</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 Live Media Streaming in Contact Flows (p. 40).</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Added content about agent queues</td>
<td>You can use agent queues to route calls directly to a specific agent. For more information, see Transfer Calls Directly to a Specific Agent (p. 28).</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, Phone Numbers for Amazon Connect in the Asia Pacific (Tokyo) Region (p. 13).</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 Use Agent Event Streams to Determine Agent ACW Time (p. 88).</td>
<td>October 30, 2018</td>
</tr>
<tr>
<td>Added troubleshooting and best practices</td>
<td>Amazon Connect Troubleshooting and Best Practices (p. 123) 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 Service-Linked Roles for Amazon Connect (p. 82).</td>
<td>October 17, 2018</td>
</tr>
<tr>
<td>Added information about queue to queue transfers</td>
<td>You can use the new options of the <strong>Transfer to queue</strong> block</td>
<td>July 31, 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 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 Initiate an Outbound Call (p. 26).</td>
<td>July 2, 2018</td>
</tr>
<tr>
<td>Added information about contact attributes and the Get queue metrics block</td>
<td>For more information, see Amazon Connect Contact Attributes (p. 46).</td>
<td>June 18, 2018</td>
</tr>
<tr>
<td>Added information about new metrics sent to Amazon CloudWatch Logs.</td>
<td>CloudWatch Metrics for Your Amazon Connect Instance (p. 100) includes additional metrics.</td>
<td>April 19, 2018</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 for Identity Management in 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 Assign Permissions to Listen to Calls (p. 69).</td>
<td>December 10, 2017</td>
</tr>
<tr>
<td>Added information about contact flow logs</td>
<td>For more information, see Contact Flow Logs (p. 97).</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about contact flow import/export</td>
<td>For more information, see Contact Flow Import/Export (p. 62).</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. 88).</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. 11).</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Added information about Login/Logout reports</td>
<td>For more information, see Login/Logout Reports (p. 84).</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>