<table>
<thead>
<tr>
<th>Release Notes</th>
<th>235</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Resources</td>
<td>234</td>
</tr>
<tr>
<td>Limits</td>
<td>231</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>225</td>
</tr>
<tr>
<td>Use the CCP (Agent's UI)</td>
<td>208</td>
</tr>
<tr>
<td>Launch the CCP</td>
<td>209</td>
</tr>
<tr>
<td>Log In and Log Out of the CCP</td>
<td>209</td>
</tr>
<tr>
<td>Log Out of the CCP</td>
<td>210</td>
</tr>
<tr>
<td>Set Your Status to Available</td>
<td>211</td>
</tr>
<tr>
<td>Chat with Contacts</td>
<td>211</td>
</tr>
<tr>
<td>What Do the Timers at the Top of the Chat Tabs Mean?</td>
<td>213</td>
</tr>
<tr>
<td>What Happens to Missed Chats?</td>
<td>214</td>
</tr>
<tr>
<td>Transfer Chats to Another Queue or Agent</td>
<td>215</td>
</tr>
<tr>
<td>Call Another Agent While on a Chat</td>
<td>218</td>
</tr>
<tr>
<td>Accept Incoming Calls</td>
<td>218</td>
</tr>
<tr>
<td>Transfer Calls</td>
<td>220</td>
</tr>
<tr>
<td>Initiate a Quick Connect Transfer</td>
<td>220</td>
</tr>
<tr>
<td>Initiate a Manual Transfer</td>
<td>220</td>
</tr>
<tr>
<td>Manage Transfer a Call</td>
<td>223</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>225</td>
</tr>
<tr>
<td>Use the Check Connectivity Tool</td>
<td>225</td>
</tr>
<tr>
<td>Common CCP Issues</td>
<td>225</td>
</tr>
<tr>
<td>Useful Troubleshooting Tools and Information</td>
<td>226</td>
</tr>
<tr>
<td>Gathering Helpful Information using the Streams API</td>
<td>227</td>
</tr>
<tr>
<td>Example Agent Issue Report Disposition</td>
<td>227</td>
</tr>
<tr>
<td>Analyzing the Data</td>
<td>227</td>
</tr>
<tr>
<td>Validation Testing</td>
<td>228</td>
</tr>
<tr>
<td>PSTN and Agent Connection Latency</td>
<td>228</td>
</tr>
<tr>
<td>Limits</td>
<td>231</td>
</tr>
<tr>
<td>Amazon Connect API Throttling Limits</td>
<td>233</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>234</td>
</tr>
<tr>
<td>Amazon Connect Service API Documentation</td>
<td>234</td>
</tr>
<tr>
<td>Amazon Connect Participant Service API</td>
<td>234</td>
</tr>
<tr>
<td>Amazon Connect Streams</td>
<td>234</td>
</tr>
<tr>
<td>Amazon Connect Chat SDK and Sample Implementations</td>
<td>234</td>
</tr>
<tr>
<td>Release Notes</td>
<td>235</td>
</tr>
<tr>
<td>November 2019 Update</td>
<td>235</td>
</tr>
<tr>
<td>Omnichannel Support</td>
<td>235</td>
</tr>
<tr>
<td>Metrics</td>
<td>235</td>
</tr>
<tr>
<td>Contact Flows</td>
<td>235</td>
</tr>
<tr>
<td>User Management</td>
<td>235</td>
</tr>
<tr>
<td>Live Media Streaming</td>
<td>235</td>
</tr>
<tr>
<td>API</td>
<td>236</td>
</tr>
<tr>
<td>Contact Control Panel (CCP)</td>
<td>236</td>
</tr>
<tr>
<td>October 2019 Update</td>
<td>236</td>
</tr>
<tr>
<td>Metrics</td>
<td>236</td>
</tr>
<tr>
<td>June 2019 Update</td>
<td>236</td>
</tr>
</tbody>
</table>
What Is Amazon Connect?

Amazon Connect is a cloud-based contact center solution. Amazon Connect makes it more efficient to set up and manage a customer contact center. It lets you 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 engaging with your customers.

You can create personalized experiences for your customers using omni-channel communications. For example, you can dynamically offer chat and voice contact based on such factors as customer preference and estimated wait times. Agents, meanwhile, conveniently handle all customers from just one interface.

Amazon Connect provides metrics and real-time reporting so you can optimize contact routing. You can also resolve customer issues more efficiently by connecting customers with the agents that can best assist them. 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. 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**—The ability to add users, such as agents or managers, and configure them with permissions that are appropriate to their roles. 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)**—A customizable interface that agents use to engage with contacts across multiple channels, such as voice and chat.
- **Contact flows**—Features that let you define 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**—The routing of contacts based on the skills of the agents.
- **Metrics and reporting**—Real-time and historical information about the activity in your contact center.

Supported Browsers

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

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>How to check your version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest 3 versions</td>
<td><a href="#">Open Chrome and type chrome://version in your address bar. The version is in the Google Chrome field at the top of the results.</a></td>
</tr>
<tr>
<td>Mozilla Firefox ESR</td>
<td>Latest 3 versions</td>
<td><a href="#">Open Firefox. On the menu, choose the Help icon and then choose About Firefox. The version number is listed underneath the Firefox name.</a></td>
</tr>
</tbody>
</table>
## Related Services

To help provide a useful customer connection experience, you can use Amazon Connect with the following services:

- **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. The user and identity management that is available in Amazon Connect is based on this service.

- **Amazon S3**—Amazon Simple Storage Service (Amazon S3) stores data from Amazon Connect, such as recordings of conversations and metrics reports.

- **AWS Lambda**—Lambda lets you 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 voice and text capabilities. 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 use the data stream to publish CTRs to Amazon Redshift, an AWS data warehouse service, or your custom data warehouse systems. You can then enable detailed analysis and reporting on your contact center 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, the number of failed and missed calls, and contact flow errors. You can set up monitors on these metrics to stay on top of the health of your contact center. For more information, see CloudWatch Metrics for Your Amazon Connect Instance (p. 165).

- **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.

### Related Services

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>How to check your version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>Latest 3 versions</td>
<td>Open Firefox. On the menu, choose the Help icon and then choose <strong>About Firefox</strong>. The version number is listed underneath the Firefox name.</td>
</tr>
</tbody>
</table>
• **AWS Key Management Service**—Amazon Connect is integrated with AWS KMS to protect your customer data. You can perform crucial management tasks 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

Use these steps to set up your contact center.

1. Create an Amazon Connect Instance (p. 27). Use an instance to contain all the resources and settings related to your contact center. You specify where voice recordings and chat transcripts are stored, and how you plan to manage user accounts and other aspects.

2. Set Up Phone Numbers for Your Contact Center (p. 33). If you’re using voice, either claim a phone number that AWS provides, or port your current phone number to Amazon Connect. If you choose to port your numbers, we suggest claiming a number so you can test Amazon Connect and build your contact center while waiting for your numbers to be ported over.

3. Set Up Routing (p. 39). Create your queues and routing profiles, and set your hours of operation. In your routing profiles, specify the channels that agents should use: voice, chat, or both. You also specify how many chats an agent can manage at the same time.

4. Create Amazon Connect Contact Flows (p. 51). Establish a contact flow to define the customer experience with your contact center from start to finish. A single contact flow works for both voice and chat, which makes your design more efficient. When you build contact flows and configure the blocks, indicate how the flow should work for voice, chat, or both.

5. Add users, which are your managers and agents, and configure their settings. Assign a routing profile to each agent, specify whether they are using a softphone or desk phone, and set how long they have for After contact work. For instructions, see Add Users (p. 135) and Set Up Agents (p. 43).

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

Next Steps

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

1. Set Up Recording Behavior (p. 69). Monitor live conversations and review past conversations. This is a way that managers can coach agents and help them improve. For voice conversations, set up recording in your contact flows. For chat conversations, set up recording at the instance level.

   To learn how to monitor conversations, see Monitor Live Conversations (p. 143).

2. Add an Amazon Lex Bot (p. 108). Use Amazon Lex in your contact center to reduce the load on your agents. For example, a bot can handle the initial interaction before the chat is routed to an agent, and also answer common questions for the customer.
Concepts

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

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

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

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

This section explains concepts that will help you set up your Amazon Connect contact center, whether you use one channel or two.

Contents

- Telephony (p. 5)
- Chat (p. 8)
- Routing Profiles (p. 11)
- Queue-Based Routing (p. 13)
- Channels and Concurrency (p. 14)
- Contact Flows (p. 15)

Telephony

Amazon Connect provides a variety of choices to enable your company to make and receive telephone calls. One of the great advantages of Amazon Connect is AWS manages the telephony infrastructure for you: carrier connections, redundancy, and routing. And, it's designed to scale.

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

Contents

- Telephony Architecture (p. 5)
- Toll-Free Numbers (p. 6)
- Direct-In-Dial (DID) Numbers (p. 6)
- Claiming Numbers in Amazon Connect (p. 7)
- Porting Numbers (p. 7)
- Use Cases for Different Configurations (p. 7)
of supported countries and costs, including the price differences between DID and toll-free numbers can be found on the Amazon Connect pricing page.

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

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

Toll-Free Numbers

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

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

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

Direct-In-Dial (DID) Numbers

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

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

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

Because DID numbers are threaded to single carrier, Amazon Connect doesn't offer carrier redundancy for DID numbers. We do offer link redundancy across multiple availability zones, so in the event of a link failure that carrier still has facilities available in another location to deliver calls. DID numbers also have a capacity limitation on how many calls a single number can accommodate, and this number does vary by region. It is important to work with your AWS account team to ensure you are properly enabled with the right type of DID numbers if you plan on using DID numbers as your primary inbound channel, and have an expectation of over 100 concurrent calls per number.
DID numbers are less expensive than toll-free numbers, but don’t have the redundancy and broad geographical coverage of a toll-free number. The ability to localize numbers may be an attractive option for your business.

Claiming Numbers in Amazon Connect

Amazon Connect provides you the ability to claim both direct dial and toll-free numbers in supported countries from inventories maintained by AWS. To claim a number, log into your Amazon Connect instance and select **Phone numbers**. For instructions, see Claim a Phone Number (p. 33).

Porting Numbers

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

If you are trying to port a number outside of the United States, follow the porting process (p. 34) we’ve documented, however, the timeline to complete may vary. If porting is not possible at all, AWS support will let you know that it’s not available.

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

For detailed porting instructions, see Port Your Current Phone Number (p. 34).

Use Cases for Different Configurations

Starting Fresh with Amazon Connect

In this case, simply select new numbers using the claim a number process. For instructions, see Claim a Phone Number (p. 33).

Migrating to Amazon Connect from Another Provider/Platform

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

- A best practice is to forward your existing numbers to a new number (or numbers) claimed in Amazon Connect until you are fully converted.
- Once fully converted, use the porting process (p. 34) to bring your numbers into Amazon Connect.
- This gives you a fallback in case you have migration issues.

Maintaining Two Separate Platforms

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

- Choose which platform is the initial call-handling service, and forward to the other platform.
• If Amazon Connect is the primary call handling platform, you can port or claim numbers. You will design your contact flows to transfer calls to the other platform on a telephone number you will provide in the contact flow.

• If the third-party platform is the primary call handler, you will need to configure that platform to forward calls to a number you claim in Amazon Connect. Choose either a toll-free number, which will give you better redundancy and capacity at an increased cost, or a bank of DID numbers to terminate the call into Amazon Connect.

• For use case we recommend you engage AWS Solution Architecture support to ensure your contact center is well-architected to achieve the best possible outcomes.

Chat

Amazon Connect allows your customers to start a chat with an agent or Amazon Lex bot, step away from it, and then resume the conversation again. They can even switch devices and continue the chat. It’s an asynchronous interaction. Learn more.

Example Chat Scenario

Suppose a customer and agent are chatting, but then the customer stops responding to the agent. The agent asks "Are you there?" and doesn’t get a reply. The agent leaves the chat. Now the chat is no longer associated with an agent; your contact flow determines what happens next.

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

Here’s how you build this scenario:

1. Create a disconnect flow. The following image shows the Sample Disconnect Flow (p. 55).
2. In the disconnect flow, add a Wait (p. 82) block. The Wait block has two branches:

- **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. The total duration of the chat, including multiple Wait blocks, cannot exceed 25 hours.
  
  For example, for this branch you might just want to run a Disconnect block and end the chat.

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

3. In your inbound contact flow, add the Set Disconnect Flow (p. 79) block. Use it to specify that when the agent or Amazon Lex bot has disconnected from the chat and only the customer remains, the set disconnect flow should run.

   In the following block, for example, we specified that the **Sample disconnect flow** should run.
When Do Chats End?

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

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

To specify wait time a shorter than 25 hours, use the **Wait** block. For example, you might wait 12 hours for the customer to resume the chat. If the customer tries to resume the chat after 12 hours, in the flow you can have an Amazon Lex bot ask if they're contacting you about the same issue or a different one.

By specifying a shorter wait time, you'll ensure customers have a good experience. Otherwise, it's possible for the customer to resume a chat after 24 hours and 58 minutes, and then be cut off after two minutes because the conversation ends automatically at the 25 hour limit.

**Tip**

If you're using Amazon Lex with chat, note that the default session timeout for an Amazon Lex session is 5 minutes. The total duration for a session can't exceed 24 hours. To change the session timeout, see Setting the Session Timeout in the Amazon Lex Developer Guide.

Enabling Your App for Chat

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

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

- Amazon Connect Service API Documentation, especially the StartChatConnect API.
- Amazon Connect Participant Service API.
- Amazon Connect Streams. Use to integrate your existing apps with Amazon Connect. You can embed the Contact Control Panel (CCP) components into your app.
- Amazon Connect Chat SDK and Sample Implementations

**Chat Initiation Method: API**

The StartChatConnect API is used to start the chat.

When you start exploring the chat experience for the first time, you'll notice that chats aren't counted in the Contacts Incoming metric in your historical metrics report. This is because the initiation method for the chat in the Contact Trace Record (CTR) is API.

![Contact Trace Record](image)

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

**More Information**

To learn more about chat, check out the following topics:

- Test a Voice or Chat Experience (p. 32)
- How Routing Works with Multiple Channels (p. 40)
- Create a Routing Profile (p. 42)
- Amazon Connect Chat SDK and Sample Implementations

**Routing Profiles**

A routing profile determines what types of contacts an agent can receive and the routing priority.
Each agent is assigned to one routing profile.
A routing profile can have multiple agents assigned to it.

Amazon Connect uses routing profiles to allow you to manage your contact center at scale. To quickly change what a group of agents does, you only need to make an update in one place: the routing profile.

Routing Profiles Link Queues and Agents

When you create a routing profile, you specify:

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

Queues: Priority and Delay

Priority and delay are powerful features that allow you to load balance contacts among groups of agents.

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

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

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

The following illustration shows you can:

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

If there are no calls in the Sales queue, then the agents will be presented with a support call.

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

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

These agents will always get sales contacts first, but if a support contact ages past 30 seconds, they will also be presented with the support contact because they are the same priority.

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

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

This routing profile prioritizes Tier 1 Support and Tier 2 Support equally because each has a priority 1.

- Agents may take contacts for Tier 3 Support when:
  - Customers for Tier 3 Support are waiting for 20 seconds or longer.
  - And no Tier 1 Support or Tier 2 Support contacts are in queue.
- Agents may take contacts for Tier 4 Support when:
  - Customers for Tier 4 Support are waiting 80 seconds or longer.
  - And no contacts for Tier 1 Support, Tier 2 Support or Tier 3 Support are in queue.
• Assign the same routing profile to multiple agents.
• Assign multiple queues to a routing profile.
• Assign a queue to multiple routing profiles.

To set up queue-based routing:

• Create the queues (p. 40), for example, one for each skill you want to use for routing.
• Create the routing profiles (p. 42):
  • Specify the channels supported by this routing profile.
  • Specify the queues: the channel, priority, and delay.
• Configure agent settings (p. 45) to assign the routing profiles to them.

When you build your contact flows, you’ll add the queues to them. If a contact chooses to speak to an agent in Spanish, for example, they will get routed to the Spanish Reservations queue.

Channels and Concurrency

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

Suppose an agent is configured in their routing profile for voice and up to 5 chats. When the agent logs in, they can be routed a chat or a voice call. However, once they are on a voice call, no more voice calls or chats are routed to them until they finish the call.
If the agent accepts a chat first, up to 5 chats will be routed to them, but no voice calls. Once they are done with the chats, they’re available for the next contact, which can be voice or chat. To learn more, see How Routing Works (p. 39).

To learn more about what the agent experiences in the Contact Control Panel when handling multiple chats, see Chat with Contacts (p. 211).

Contact Flows

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

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

Default Contact Flows

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

When you customize your contact center and create new flows, you’re replacing the default contact flows with your own.

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

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

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

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

Contact Flow Designer

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

Contact Blocks

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

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

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

For a list of the available contact blocks and descriptions about what they do, see **Contact Block Definitions (p. 72).**

**Sample Contact Flows**

To see how to put contact blocks together to create different flows, see **Sample Contact Flows (p. 53).**
Best Practices for Amazon Connect

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

Contact Flows

- Use consistent attribute naming conventions across all AWS services. Use camel case for yourAttributeNames to avoid confusion when passing and referencing variables.
- Use standard naming conventions for attribute names. Don't use spaces or special characters that could impact downstream reporting processes such as AWS Glue crawlers.
- Create modular contact flows. Make the flows as small as possible, and then combine modular flows into an end-to-end contact experience. This helps to keep your flows manageable, and you won't require numerous regression testing cycles.
- Ensure all error branches are routed to a block that effectively handles the error or terminates the contact.
- Use a Set logging behavior block to enable or disable logging for segments of the contact flow where sensitive information is collected and can't be stored in CloudWatch.
- Use Set recording behavior block in your contact flow to disable and enable recordings according to your use case. Keep in mind that Amazon Connect records conversations with agents only. It doesn't record IVR interactions.
- Ensure that attributes used in the flow are set and referenced correctly. If there are periods prepended to the attribute names, you are likely using JSONPath ($.) format while also selecting a variable type from the pick list. For example, using:
  - Save text as attribute and value $.External.variableName works as expected.
  - Use attribute and value variableName works as expected.
  - Use attribute and $.External.variableName results in a prepended period.
- Before transferring a call to agent and putting that call in a queue, ensure that Check hours of operation and Check staffing blocks are used. They verify that the call is within working hours and that agents are staffed to service.
- Ensure that callbacks are offered before and after queue transfer by using Check queue status blocks. Include a condition for Queue capacity that is greater than X, where X is a number representing your expected queue capacity.
  - If queue capacity exceeds the expected capacity, use a Get Customer Input block to offer a callback. This retains the caller's position in the queue and calls them back when an agent is available.
  - In the Set callback number block, choose the number to be used to call the customer back in the CCP. Use System and Customer Number or a new number, collected by a Store Customer Input block, using System and Stored customer input.
  - Finally, add a Transfer to queue block. Configure it to Transfer to callback queue and configure the callback options to fit your specific use case.
- Use a Loop prompts block in your Customer queue flow to interrupt with a queued callback and external transfer option at regular intervals.
- Ensure that all countries referenced in external transfers or used for outbound dialing are added to the service limit for your account/instance.
- Ensure that all numbers referenced in external transfers are in E.164 format. Drop the national trunk prefix that you use when calling locally. This prefix would be the leading 0 for most of Europe, 1 for
the US. The prefix is replaced by the country code. For example, the UK mobile number 07911 123456 in E.164 format is +44 7911 123456 (tel:+447911123456).

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

User Access and Security Profiles

- Ensure that all profile permissions are as restrictive as possible. Allow access to only those resources absolutely required for the user's role. For example, don't give agents permissions to create, read, or update users in Amazon Connect.
- Ensure that multi-factor authentication (MFA) is set up through your SAML 2.0 identity provider, or Radius server, if that's more applicable for your use case. After MFA is set up, a third text box becomes visible on the Amazon Connect login page to provide the second factor.
- If you use an existing directory through AWS Directory Service or SAML-based authentication for identity management, ensure that you follow all security requirements appropriate for your use case.
- Use the Login as administrator button on the instance page of the AWS console only in emergency scenarios. For example, use this option if you can't otherwise access the system because no administrator credentials or accounts with administrator permissions are available. Do not use the administrator login to manage your contact center.

Lambda

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

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

Chat and Amazon Lex

- You can use the same bot for both the voice and chat channels. However, you may want the bot to respond differently based on the channel. For example, you want to return SSML for voice so a number is read as a phone number, but you want to return normal text to chat. You can do this by passing the Channel attribute. For instructions, see How to Use the Same Bot for Voice and Chat (p. 95).
- For voice, some words are best spelled phonetically to get the correct pronunciation, such as last names. If this is the case with your scenario, include it in the design of your bot. Or, you can keep the voice and chat bots separate.
- Tell agents about the bot. When a contact is connected to the agent, the agent sees the entire transcript in their window. The transcript includes text from both the customer and the bot.

Contact Control Panel

- If your agents use Google Chrome 71 to Chrome 75, and they use chat, add the CCP URL to the allow list in the agent's Chrome settings. Otherwise, they won't hear the audio indicator notifying them that there's an incoming chat.
For instructions, see this Google Chrome Help article.
Plan Your Identity Management in Amazon Connect

Before you set up your Amazon Connect instance (p. 27), you should decide how you want to manage your Amazon Connect users. You cannot change the option you select for identity management after you create the instance.

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

When you create your instance, you'll be prompted to choose from one of the following identity management solutions supported in Amazon Connect:

- **Store users with Amazon Connect**—Choose this option if you want to create and manage user accounts within Amazon Connect. 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. 20).

- **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. 21).

Use an Existing Directory for Identity Management

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

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

- **Microsoft Active Directory**—AWS Directory Service lets you run Microsoft Active Directory as a managed service.

- **Active Directory Connector**—AD Connector is a directory gateway you can use to redirect directory requests to your on-premises Microsoft Active Directory.

- **Simple Active Directory**—Simple AD is a standalone managed directory that is powered by a Samba 4 Active Directory compatible server.
You cannot change the identity option you select after you create the instance. If you decide to change the directory you selected, you can delete the instance and create a new one. When you delete an instance, you lose all configuration settings and metrics data for it.

There is no additional charge for using an existing or a proprietary directory in Amazon Connect. For information about the costs associated with using AWS Directory Service, see AWS 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 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. 21)
- Enabling SAML-based Authentication for Amazon Connect (p. 22)
- Select SAML 2.0-based Authentication During Instance Creation (p. 23)
- Enable SAML Federation Between Your Identity Provider and AWS (p. 23)
- Use a Destination in Your Relay State URL (p. 25)
- Add users to Your Amazon Connect Instance (p. 25)
- SAML User Logging in and Session Duration (p. 26)

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

   **Important**
   Replacing this role can cause previously federated users to fail at federation.

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

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

1. On the Attach permissions policy page, choose Create policy.
2. On the Create policy page, choose JSON.
3. Copy one of the following example policies and paste it into the JSON policy editor, replacing any existing text. You can use either policy to enable SAML federation, or customize them for your specific requirements.
Use this policy to enable federation for all users in a specific Amazon Connect instance. For SAML-based authentication, replace the value for the `Resource` to the ARN for the instance that you created:

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

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

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement2",
         "Effect": "Allow",
         "Action": "connect:GetFederationToken",
         "Resource": "*",
         "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:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement2",
         "Effect": "Allow",
         "Action": "connect:GetFederationToken",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "connect:InstanceId": [
                  "2fb42df9-78a2-2e74-d572-c8af67ed289b",
                  "1234567-78a2-2e74-d572-c8af67ed289b"
               ]
            }
         }
      }
   ]
}
```
4. After you create the policy, choose Next: Review. Then return to step 10 in the To create a role for SAML-based federation procedure in the Creating a Role for SAML 2.0 Federation (Console) topic.

3. Configure your network as a SAML provider for AWS. For more information, see Enabling SAML 2.0 Federated Users to Access the AWS Management Console.

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

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

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

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

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

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

**Use a Destination in Your Relay State URL**

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

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

**Add users to Your Amazon Connect Instance**

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

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

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

SAML User Logging in and Session Duration

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

As a best practice, you should also define a process for your Amazon Connect users to log out when they are finished using Amazon Connect. They should log out from both Amazon Connect and your identity provider. If they do not, the next person that logs in to the same computer can log in to Amazon Connect without a password since the token for the previous sessions is still valid for the duration of the session, by default, 10 hours.

About session expiration

Amazon Connect sessions expire 10 hours after a user logs in. After 10 hours, users are automatically logged out, even if they are currently on a call. If your agents stay logged in for more than 10 hours, they need to refresh the session token before it expires. To create a new session, agents need to log out of Amazon Connect and your IdP and then log in again. This resets the session timer set on the token so that agents are not logged out during an active contact with a customer. When a session expires while a user is logged in, the following message is displayed. To use Amazon Connect again, the user needs to log in to your identity provider.

![Session expired](image)
Set Up Your Contact Center

Amazon Connect enables you to create a virtual contact center in the AWS cloud. To get started, create a virtual contact center instance. For more information, see Get Started with Amazon Connect (p. 4).

After you create an instance, you can edit its settings, such as telephony, data storage, and data streaming. After that, you can assign your contact center a phone number or import your own phone number. You can add agents to your contact center, and assign them permissions appropriate to their roles. You can set up a single queue for incoming contacts, or set up multiple queues so that you can route contacts to agents with specific skills.

A key part of setting up your contact center is to define how your customers experience it. You do this by creating contact flows.

Finally, you'll need to provide your agents access to the Contact Control Panel (CCP), which they will use to interact with contacts.

Contents
• Create an Amazon Connect Instance (p. 27)
• Test a Voice or Chat Experience (p. 32)
• Set Up Phone Numbers for Your Contact Center (p. 33)
• Set Up Routing (p. 39)
• Set Up Agents (p. 43)
• Provide Access to the Contact Control Panel (p. 47)

Create an Amazon Connect Instance

The first step in setting up your Amazon Connect contact center is to create a virtual contact center instance. Each instance contains all the resources and settings related to your contact center.

You might want to create multiple contact center instances, for example, one as a Sandbox for development, another for QA, and a third for Production. Settings, users, metrics, and reporting aren't shared among instances.

Each instance functions only within the AWS Region in which you create it.

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 Plan Your Identity Management in Amazon Connect (p. 20).

**To configure identity management for your instance**

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose Get started. If you have previously created an instance, choose Add an instance instead.
3. Choose one of the following options:
   - **Store users within Amazon Connect** - Use Amazon Connect to create and manage user accounts.
   - **Link to an existing directory** - Use an AWS Directory Service directory to manage your users. You can use each directory with one Amazon Connect instance at a time.
   - **SAML 2.0-based authentication** - Use an existing identity provider (IdP) to federate users with Amazon Connect.
4. If you chose Store users within Amazon Connect or SAML 2.0-based authentication, provide the left-most label for Access URL. This label must be unique across all Amazon Connect instances in all Regions. You can't change the access URL after you create your instance.
5. If you chose Link to an existing directory, select the AWS Directory Service directory for Directory. The directory name is used as the left-most label for Access URL.
6. Choose Next step.

**Step 2: Administrator**

After you specify the user name of the administrator for the Amazon Connect instance, a user account is created in Amazon Connect and the user is assigned the Admin security profile.

**To specify the administrator for your instance**

1. Do one of the following, based on the option that you chose in the previous step:
   - If you chose Store users within Amazon Connect, select Add a new admin, and provide a name, password, and email address for the user account in Amazon Connect.
   - If you chose Link to an existing directory, for Username, type the name of an existing user in the AWS Directory Service directory. The password for this user is managed through the directory.
   - If you chose SAML 2.0-based authentication, select Add a new admin and provide a name for the user account in Amazon Connect. The password for this user is managed through the IdP.
2. Choose Next step.

**Step 3: Telephony Options**

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 reports and recordings of conversations, 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 recordings of conversations and exported reports. Alternatively, you can specify separate buckets and keys for recordings of conversations and exported reports.

By default, we enable call recording, chat transcripts, exported reports, and contact flow logs. Live media streaming is not enabled by default.

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 or enable/disable certain functionality:

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

Step 5: Review and Create

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

To create your instance

1. Review the configuration choices. Remember that you cannot change the identity management options after you create the instance.
2. (Optional) To change any of the configuration options, choose Change.
3. Choose Create instance.
4. (Optional) To continue configuring your instance, choose Get started and then choose Let's go. If you prefer, you can access your instance and configure it later on. For more information, see Next Steps (p. 29).

If you chose to manage your users directly within Amazon Connect or through an AWS Directory Service directory, you can access the instance using its access URL. If you chose to manage your users through SAML-based authentication, you can access the instance using the IdP.

Next Steps

After you create an instance, you can assign your contact center a phone number or import your own phone number. For more information, see Set Up Phone Numbers for Your Contact Center (p. 33).
Create Another Instance

To create another instance

1. In the AWS Management Console, choose Amazon Connect.
2. Choose Add an instance.
3. Complete the steps on the Amazon Connect resource configuration page. For instructions see Create an Amazon Connect Instance (p. 27).

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 recordings of voice conversations, choose Call recordings, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
3. (Optional) To specify the bucket and KMS key for recordings (transcripts) of chat conversations, choose Chat transcripts, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.
4. (Optional) To enable live media streaming, choose Live media streaming, Edit. For more information, see Capture Customer Audio: Live Media Streaming (p. 122).
5. (Optional) To specify the bucket and KMS key for exported reports, choose Exported reports, Edit, specify the bucket name and prefix, select the KMS key by name, and then choose Save.

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. 31).
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 Encrypt Customer Input (p. 121).
3. (Optional) To integrate with Amazon Lex, select a Lex bot. For more information, see Add an Amazon Lex Bot (p. 108).
4. (Optional) To integrate with AWS Lambda, select a Lambda function. For more information, see Invoke Lambda Functions (p. 117).
5. (Optional) To enable contact flow logs, choose Enable contact flow logs. For more information, see Contact Flow Logs (p. 163).

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 recordings of conversations 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 scheduled reports or recordings of conversations. For more information, see Creating Keys in the AWS Key Management Service Developer Guide.

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.

Test a Voice or Chat Experience

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

To test voice: once you claim a number you can immediately call it to hear what the experience will be like for your customers. Amazon Connect uses the default contact flows (p. 51) to power your initial experience. To test a customized contact flow, assign a phone number (p. 61) to it and then call that number.

To test chat: Amazon Connect includes a simulated web page that shows how your customers can interact with you, and a Contact Control Panel (CCP) that shows the agent experience. Here's how to test chat:

1. Go to the Amazon Connect Dashboard, and choose Test chat.
   
   If you don't see the option to test chat, click here.
2. On the Test Chat page, choose Test Settings.
3. Under System Settings, choose the contact flow you want to test with chat, and then click Apply. By default, it runs the Sample Inbound Flow (p. 53).
4. In the chat window, click the icon as shown below.

5. Type a message similar to what one of your customers might type. In the agent window, type a reply.
6. To see what it's like for an agent to handle multiple chat conversations, copy the dashboard URL into another browser window, and start another chat. The chat goes to the same instance of the CCP that you already have open.

Tip
The test environment uses the BasicQueue and Basic Routing Profile. The Basic Routing Profile is set up for 2 chats. If you want to test what it's like to have more than two chats, change the Basic Routing Profile to 5 chats. For instructions, see Create a Routing Profile (p. 42).
Set Up Phone Numbers for Your Contact Center

After you create an Amazon Connect instance, you can claim a phone number to use for your contact center. You can use this phone number to place a test call in to your contact center to confirm that it is working correctly. You can also use it in your production environment.

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

If you want to keep a phone number you already have, you can port the phone number and use it with Amazon Connect.

Contents
• Claim a Phone Number (p. 33)
• Release a Phone Number (p. 34)
• Port Your Current Phone Number (p. 34)
• Claim Phone Numbers for Amazon Connect in the Asia Pacific (Tokyo) Region (p. 36)

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
   Use the Amazon Connect service limits increase form for these situations:
   • If you select a country, but there are no numbers displayed for that country, you can request additional numbers for the country.
   • If you want to request a specific area code or prefix that you don't see listed.

   We'll try to accommodate your request.
4. Enter a description for the number and, if required, attach it to a contact flow in Contact flow / IVR.
5. Choose Save.
6. Repeat this process until you have claimed all your required phone numbers.

There is a service 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.
Release a Phone Number

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

You cannot claim the same phone number after releasing it.

**Tip**
If you want to "close" your Amazon Connect account, do these steps for all of your phone numbers. This will ensure you aren't billed if people erroneously call numbers that you've claimed, and trigger your contact flows. You may also want to delete your instances. (p. 31)

To release a phone number

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose **Routing, Phone numbers**.
3. Choose the phone number you want to release, and then choose **Release**.

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

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

Port Your Current Phone Number

To continue 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 from Amazon Connect so 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.
3. Choose **Create case**.
4. Under **Create case, Case classification**, do the following:
   - For **Limit type**, choose **Amazon Connect**.
   - For **Contact Center Instance ARN - optional**, enter the instance ARN.

   To find the ARN for your instance, log in to Amazon Connect. On the instances page, click the instance alias.
This will take you to a page that displays the instance ARN.

5. Under **Requests, Request 1** do the following:
   - 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.

6. (Optional) If you want to port more phone numbers, choose **Add another request**, and then repeat step 5 for each additional request.

7. Under **Case description, Use case description**, include as much information as possible about your request, including whether the numbers are Direct Inward Dial or toll-free, your current carrier, and the contact information for the person authorized to make changes to your current phone service. If you don’t know all of these details, you may leave information out.

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

9. 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.

**Claim Phone Numbers for Amazon Connect in the Asia Pacific (Tokyo) Region**

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

**Port and Protocol Requirements for Using Amazon Connect in the Asia Pacific (Tokyo) Region**

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Transport Layer</th>
<th>IP Range</th>
</tr>
</thead>
</table>
### Protocol, Port, Transport Layer, IP Range

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

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

Amazon Connect supports the following phone numbers for instances created in the Asia Pacific (Tokyo) Region.

- **Direct Inward Dialing (DID) numbers**—DID numbers are also referred to as local numbers.
  - 050 prefix numbers.
  - 03 prefix for numbers in Tokyo. Amazon Connect does not offer phone numbers for other cities in Japan at this time.

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

- **Toll Free numbers**
  - 0120 prefix numbers.
  - 0800 prefix numbers.

  **Note**
  When you claim a toll free phone number for Amazon Connect, there is no corresponding DID number with a 03 prefix also assigned, as with other toll free numbers in Japan. If you need to use a DID number, you can claim one in Amazon Connect.

### How to Claim a Phone Number for Amazon Connect Instances in the Asia Pacific (Tokyo) Region

You can claim a 050 prefix number directly within Amazon Connect. If you plan to use a number with a 03 prefix from Tokyo, pursuant to Japanese regulatory requirements, you must submit an Amazon Connect service 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.
- 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.

Set Up Routing

In Amazon Connect, routing consists of three parts: queues, routing profiles, and contact flows. This topic discusses queues and routing profiles. For information about contact flows, see Create Amazon Connect Contact Flows (p. 51).

A queue holds contacts waiting to be answered by agents. You can use a single queue to handle all incoming contacts, or you can set up multiple queues.

Queues are linked to agents through a routing profile. When you create a routing profile, you specify:

- Which queues will be in it.
- Whether one queue should be prioritized over another.
- What channels agents will handle in the Contact Control Panel (CCP): voice, chat, or both.
- How many chat conversations agents can handle simultaneously, up to 5.
- Whether individual queues are for voice, chat, or both.

Each agent is assigned to one routing profile.

Contents

- How Routing Works (p. 39)
- Create a Queue (p. 40)
- Set the Hours of Operation for a Queue (p. 41)
- Set Up Outbound Caller ID (p. 41)
- Create a Routing Profile (p. 42)

How Routing Works

Contacts are routed through your contact center based on these factors:

- The routing profile an agent is assigned to.
- The hours of operation for a given queue.
• The routing logic you define in your contact flows.

For example, you use routing profiles to route specific types of contacts to agents with specific skill sets. If no agent with the required skill set is available, you can place the contact in the queue defined in the contact flow.

Here's the logic Amazon Connect uses to route contacts:

• Contacts in a queue are automatically prioritized and forwarded to the next available agent.
• Contacts are placed on hold if there are no available agents. The order in which they are serviced is determined by their time in queue, on a first-come, first-served basis.
• If multiple agents are available, the contact is routed to the agent who has been in the Available status for the longest time.
• A routing profile may assign a priority to one queue over another, but the priority within the queue is always set by the order the contact was added to the queue.

How Routing Works with Multiple Channels

When you set up a routing profile to handle both voice and chat channels, agents must complete the interactions with inbound contacts on one channel before they can receive a contact on the other.

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

• When agents sign on, they can be routed a chat or voice contact.
• After the agents begin interacting with a voice contact, no chats or voice contacts are routed to them until they finish the call.
• When agents accept a chat, up to 5 chats are routed to them, but no voice contacts. After they're done with the chats, they're available for the next contact, which could be voice or chat.

This routing model allows agents to handle both voice and chat channels. It routes contacts to the agent based on the type of contact the agent is already on. This way, if an agent is already chatting with a customer, it's more efficient for the agent to respond to more chats instead of multitasking on two different channels.

To learn how to set up multiple channels, see Create a Routing Profile (p. 42).

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.

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 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.
Set the Hours of Operation for a Queue

The first thing you need to do when you set up a queue is to specify the hours of operation. The hours may be referenced in contact flows. For example, when routing contacts to agents, you might use the Check hours of operation block first, and then route the contact to the appropriate queue.

To set the hours of operation for a queue

1. Choose Routing, Hours of operation.
2. To create a template, choose Add new hours and enter a name and a description.
3. For Time zone, select a value.
4. For Add new, set new hours.
5. Choose Save.

Set Up Outbound Caller ID

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

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

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

- In a queue. You can specify both the outbound caller ID name and the phone number. For instructions, see Create a Queue (p. 40).
- In the Set callback number block in a contact flow. Use this block to set up customer callback. You can only specify the phone number. For more information about this block, see Contact Block Definitions (p. 72).
- In the Call phone number block in an outbound whisper contact flow. You can use this block with the Set contact attributes block to set the callback number dynamically. For example, you can display a certain caller ID number based on the customer's account type. For more information, see Initiate an Outbound Call (p. 70).
- In the Transfer to phone number block. For more information, see Set Up Contact Transfers (p. 63).

Why Your Caller ID Might Not Appear Correctly to Customers

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

To have this work more consistently, in the US, telephony providers will likely require registering your name with CNAM databases, such as Neustar, (formerly Targus), VeriSign, or Syniverse. Amazon Connect does not support CNAM registration directly. We are considering adding CNAM registration as a feature of Amazon Connect in the future. In the interim, you can add CNAM functionality to your existing phone numbers by engaging with companies that focus specifically on accurate CNAM and fraud applications.

While we can't speak for a specific provider, Neustar has historically been used by companies such as Verizon, CenturyLink, Fairpoint, Frontier, Windstream, Comcast, Cox, and others. You can and may want
to register with multiple CNAM databases. Even so, CNAM registration is not a guarantee since not all carriers do a CNAM look up, and some charge you for it.

Create a Routing Profile

While queues are a ‘waiting area’ for contacts, a routing profile links queues to agents. When you create a routing profile, you specify which queues will be in it. You can also specify whether one queue should be prioritized over another.

Each agent is assigned to one routing profile.

To create a routing profile

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a searchable display name.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe what the routing profile is for.</td>
</tr>
</tbody>
</table>

Set channels and concurrency

Choose whether agents assigned to this profile handle contacts using voice, chat, or both.

For Chat, specify up to five chat conversations that an agent can have simultaneously.

For information about how Amazon Connect routes contacts when multiple channels are in use, see How Routing Works with Multiple Channels (p. 40).

3. Under Routing profile queues, enter the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Use the dropdown menu to choose a queue you’ve already set up. You can add multiple queues to a routing profile.</td>
</tr>
<tr>
<td>Channels</td>
<td>Choose whether the queue is for chat, voice, or both.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specify the order in which contacts are to be handled for that queue. For example, a contact in a queue with a priority of 2 would be a lower</td>
</tr>
</tbody>
</table>
Set Up Agents

You can manage and load-balance customer contacts using agent hierarchy organization and agent status management. These tools provide filtering and agent availability management per queue, skill set, and routing profiles.

Contents
- Set Up Agent Hierarchies (p. 43)
- Add Custom Agent Status (p. 44)
- Configure Agent Settings (p. 45)
- Enable Auto-Accept Call for Agents (p. 46)

Set Up Agent Hierarchies

Agent hierarchies are a way for you to organize agents into teams and groups for reporting purposes. It’s useful to organize them based on their location and their skill sets. For example, you might want to

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority than a contact in a queue with a priority of 1.</td>
<td></td>
</tr>
<tr>
<td>Delay (in seconds)</td>
<td>Enter the minimum amount of time a contact should be in the queue before they are routed to an available agent.</td>
</tr>
<tr>
<td>Default outbound queue</td>
<td>Choose a queue to be associated with outbound calls placed by the agents.</td>
</tr>
</tbody>
</table>

4. Choose Add new profile.

Tips for Setting Up Channels and Concurrency

- Use Set channels and concurrency to toggle on and off whether agents assigned to a profile get voice and chat contacts.

For example, there are 20 queues assigned to a profile. All of the queues are enabled for both voice and chat. By removing the Voice option at the routing profile level, you can stop all voice calls to these agents, across all queues in the profile. When you want to restart voice contacts for these agents again, select Voice.

- For each queue in the profile, choose whether it’s for voice or chat contacts, or both.
- If you want a queue to handle both voice and chat contacts, but want to assign a different priority to each channel, add the queue twice, like this:

<table>
<thead>
<tr>
<th>Name</th>
<th>Channels</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>BasicQueue</td>
<td>Voice</td>
<td>1</td>
</tr>
<tr>
<td>BasicQueue</td>
<td>Voice</td>
<td>2</td>
</tr>
</tbody>
</table>
create large groups, such as all agents who work on a specific continent, or smaller groups such as all agents working in a specific department.

You can also configure hierarchies with up to five levels, and segment agents or teams. Here are a couple of things to note about using hierarchies:

- Removing agents from a level affects historical reporting.
- 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 Assign Permissions: Security Profiles (p. 136).

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.

After you create a hierarchy, 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.

Add Custom Agent Status

Agents are responsible for setting their status in the Contact Control Panel (CCP). In fact, the only time an agent's status changes is when they manually change it in the CCP.

Amazon Connect provides two default status values:

- Available
- Offline

You can change the name of these values, and you can add new ones. For example, you might add a status for Lunch, and another for Training. These and the default status values will be used for reporting, metrics, and resource management.

When you add a new status, it will always be Custom, not routable.

You can't delete a status value but you can disable it so it doesn't appear on the agent's CCP.

To add a new agent status

1. Choose Users, Agent status, Add new agent status.
2. Enter a status name and description, and select whether the status should appear in the CCP to the agent.
3. Choose Save.

To change the order that the status values appear in the CCP, click the waffle next to the status value and drag it to the order you want.

<table>
<thead>
<tr>
<th>Status name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Available state</td>
</tr>
<tr>
<td>Break</td>
<td>Lunch and coffee breaks</td>
</tr>
<tr>
<td>Training</td>
<td>Training on the new tools</td>
</tr>
<tr>
<td>Offline</td>
<td>Offline state</td>
</tr>
</tbody>
</table>

To edit a status
1. Choose Users, Agent status.
2. Hover over the status name and choose the edit icon.
3. Enter the new information, and choose Save to apply the changes.

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

Configure Agent Settings

Before you configure your agent settings, here is some info to have on hand. Of course, you can always change this information later.

- What is their routing profile? They can only be assigned one.
- Will they have the Agent security profile or a custom profile you created?
- Are they going to use a soft phone? If so, will they be connected to contacts automatically, or will they need to press the Accept button in their contact control panel (CCP)?
- Or, are they going to use a desk phone? If so, what is their number?
- How long do they have for After contact work (ACW)?
- Are they going to be assigned to an agent hierarchy?

Note
You can't configure how long an available agent has to connect with a contact before it's missed.

To configure agent settings
1. In the navigation pane, go to Users, User management.
2. Choose the user you want to configure, then choose Edit.
3. Assign a routing profile (p. 42) to them. You can only assign one.
4. Assign the Agent security profile, unless you've created custom security profiles.
5. Under **Phone Type** choose whether the agent is using a desk phone or soft phone.
   - If you select desk phone, enter their phone number.
   - If you select soft phone, choose **Auto-Accept Contact** if you want agents to be connected to calls automatically. This doesn't apply to chats.

6. In **After contact work (ACW) timeout**, type how long in seconds agents have for after contact work, such as entering notes about the contact.

7. Under **Agent Hierarchy** select any groups the agent should be part of.

---

### Enable Auto-Accept Call for Agents

When Auto-Accept Call is enabled for an available agent, the agent connects to contacts automatically.

**Tip**

When a call arrives to an agent who has Auto-Accept Call enabled, the Contact Control Panel (CCP) briefly shows the options **Accept** or **Reject**. This is expected behavior. After a moment, the call is automatically accepted and these options disappear.

You can't enable Auto-Accept Call while editing multiple existing users in your Amazon Connect instance. You must edit existing users individually to enable it. You can also configure the setting for multiple new users when you bulk upload new users with the CSV template.

---

### Enable Auto-Accept Call for Existing Agents

To complete these steps, you must log in as a user who has the following permissions in their security profile: **Edit, Create, Remove, Enable / Disable, and Edit permission**.

1. Log in to your Amazon Connect instance using your access URL (https://domain.awsapps.com/connect/login).
2. In the left navigation bar, choose **Users, User management**.
3. In the list of users, select an agent, and then choose **Edit**.
4. On the Edit users page, under **Phone Type**, select the **Auto-Accept Call** check box.
5. Choose **Save**.
6. Repeat these steps for each user that you want to edit.

---

### Bulk Upload New Users with Auto-Accept Call Enabled

You can't use the CSV template to edit information for existing users. If you include duplicate users with different information in the CSV template, you will receive an error.

1. Log in to your Amazon Connect instance using your access URL (https://domain.awsapps.com/connect/login).
2. In the left navigation bar, choose **Users, User management**.
3. Choose **Add new users**.
4. Under **How do you want to set up your existing users?**, next to **Upload my users from a template (csv)**, choose **template** to download a pre-formatted CSV file.
5. In the CSV file, configure the details for the new users who you want to add. For **soft phone auto accept (yes/no)**, be sure to enter **yes**.
6. After configuring the CSV file, in your Amazon Connect instance, choose **Upload my users from a template (csv)**, and then choose **Next**.
7. Under **Select and upload a spreadsheet with user details**, choose **Choose file**.
8. Choose the configured CSV file from its location on your computer.
Provide Access to the Contact Control Panel

Agents use the Amazon Connect Contact Control Panel (CCP) to communicate with contacts. But before agents can access the CCP and handle contacts, there are a few things you need to do:

- Add them as users to the instance. For more information, see Manage Users in Amazon Connect (p. 135).
- 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 Assign Permissions: Security Profiles (p. 136).
- 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.

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

Grant Microphone Access in Chrome or Firefox

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.

For help solving problems with hearing a conversation, see Set up Softphones and Desk Phones (p. 48).

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, or if they are having problems hearing a conversation or being heard, check the following:

- **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.

Agent Workstation Requirements for the CCP

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 contacts, 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 contacts. Also, keep in mind the resource requirements when scoping workstations to ensure that they can perform under load while appropriately multitasking for the use case. For the best agent and customer audio experience, a USB headset is recommended. Alternatively, you can redirect the contact 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 for the CCP (p. 48) 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.

### Can't Hear Caller Or Caller Can't Hear Agent?

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

- The connection between the agent's headset and computer.
- The permissions for the browser microphone.

Here's what you need to check:

- **Headset connectivity**—Check the settings in Device Manager to ensure that your computer recognizes the headset and allows proper headset connectivity. For example, if you're using a Windows PC, go to **Device Manager**, then expand **Audio inputs and outputs**. If your computer recognizes your headset, you'll see it listed there.
• **Browser settings for headset/microphone**—In Chrome, go to **Settings, Site Settings, Microphone**. Then check that the correct headset is enabled. Or, in Firefox, while in the CCP, choose the lock icon in the address bar. If needed, grant permissions to the CCP. To learn more, see Use your camera and microphone in Chrome or 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.

For more information about solving audio problems, see Troubleshooting Issues with the CCP (p. 225).

**Can't Hear Indicator for Incoming Chat?**

If an agent can't hear the audio indicator for an incoming chat, the problem is likely because Google added an audio policy flag to Chrome. This flag exists in Chrome versions 71 - 75.

To fix this, add the CCP web site to the allow list in the agent's Chrome settings. For instructions, see this Google Chrome Help article.

For more information about solving audio problems, see Troubleshooting Issues with the CCP (p. 225).
Create Amazon Connect Contact Flows

A contact flow defines the customer experience with your contact center from start to finish. Amazon Connect includes a set of default contact flows (p. 51) so you can quickly set up and run a contact center. However, you may want to create custom contact flows for your specific scenario.

Contents
- Default Contact Flows (p. 51)
- Sample Contact Flows (p. 53)
- Create a New Contact Flow (p. 58)
- Associate a Phone Number with a Contact Flow (p. 61)
- Create Prompts (p. 61)
- Set Up Contact Transfers (p. 63)
- Set Up Recording Behavior (p. 69)
- Initiate an Outbound Call (p. 70)
- Import/Export Contact Flows (p. 71)
- Contact Block Definitions (p. 72)
- Use Amazon Connect Contact Attributes (p. 84)

Default Contact Flows

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

For example, say you create a contact flow that includes putting the customer on hold, but you don’t create a prompt for it. The default contact flow, Default agent hold, will be played automatically. This is a way to help you get started with your call center quickly.

Tip
- If you want to change the behavior of a default contact flow, we recommend you instead just create a new customized default with a different name than the original. Then call it intentionally in your contact flows rather than defaulting to it. This will give you better control over how your contact flows work.

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

Following is a description of each default flow.

Default Agent Hold

The default agent hold flow is the experience the agent receives when placed on hold. During this flow, a Loop prompt block plays the message “You are on hold” to the agent every 10 seconds.
Default Agent Transfer

This default transfer flow is the customer's experience when the customer is transferred to an agent by using Create Quick Connects (p. 64). A Play prompt plays the message “Transferring now.” Then the Transfer to agent block is used to transfer the contact to the agent.

Tip
The Transfer to Agent block is a beta feature and only works for voice interactions. To transfer a chat contact to another agent, follow these instructions: Using Contact Attributes to Route Contacts to a Specific Agent (p. 68).

Default Customer Queue

This default contact flow is played when a customer is placed in a queue. The loop has a one-time voice prompt and queue music in .wav format that's been uploaded to the Amazon Connect instance.

The customer remains in this loop until their call is answered by an agent.

Default Customer Whisper

This contact flow starts immediately before the call is connected. It uses a "beep" sound to notify a customer that their call has been connected to an agent.

Default Agent Whisper

This contact flow plays for the agent immediately before the call is connected with the customer. This type of flow can be used to play a prompt for the agent.

The name of the queue is played to the agent. It identifies for the agent the queue that the customer was in. The name of the queue is retrieved from the system variable $.Queue.Name.

For more information about system variables, see Contact Flow System Attributes (p. 97).

Default Customer Hold

This contact flow starts when the customer is put on hold. It plays the audio that the customer hears while on hold.

Default Outbound

This contact flow is an outbound whisper that manages what the customer experiences as part of an outbound call, before being connected with an agent.

It starts with an optional Set recording behavior block. Then a prompt plays indicating the call isn't being recorded, and the flow ends.

The customer remains in the system (on the call) after the flows ends.

Default Queue Transfer

This contact flow is manages what the customer experiences when they are transferred to another queue.

It starts with a Check hours of operation block to check the hours of operation for the current queue. The In hours option branches to the Check staffing block to determine whether agents are available, staffed, or online.
If it returns True (agents are available), the flow goes to the Transfer to queue block. If it returns False (no agents are available), the flow plays a prompt and disconnects the call.

Sample Contact Flows

Amazon Connect includes a set of sample contact flows that show you how to perform common functions. They are designed to help you learn how to create your own contact flows that work in a similar way. For example, if you want to add a queued callback flow to your call center, take a look at the Sample Queued Callback (p. 55) flow.

To explore how the sample flows work

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

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

To open a sample flow in the contact flow designer

1. In Amazon Connect choose Routing, Contact flows.
2. On the Contact flows page, scroll down to the flows with names that start with Sample.
3. Choose the flow you want to view.

The topics in this section describe how each of the sample contact flows work.

Contents

- Sample Inbound Flow (First Contact Experience) (p. 53)
- Sample AB Test (p. 54)
- Sample Customer Queue Priority (p. 54)
- Sample Disconnect Flow (p. 55)
- Sample Queue Customer (p. 55)
- Sample Queued Callback (p. 55)
- Sample Queue Configurations (p. 55)
- Sample Interruptible Queue Flow with Callback (p. 56)
- Sample Lambda Integration (p. 56)
- Sample Recording Behavior (p. 57)
- Sample Note for Screenpop (p. 57)
- Sample Secure Input with Agent (p. 57)
- Sample Secure Input with No Agent (p. 58)

Sample Inbound Flow (First Contact Experience)

Type: Contact flow (inbound)
This sample flow is automatically assigned to the phone number that you claimed when you first set up contact flows. For more information, see Get started (p. 4).

It uses Check contact attributes to determine if the customer is contacting you by phone or chat, and to route them accordingly.

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

**Sample AB Test**

Type: Contact flow (inbound)

This contact flow shows how to perform an A/B call distribution based on a percentage. Here's how it works:

1. The Play prompt block uses Amazon Polly, the text-to-speech service, to say "Amazon Connect will now simulate rolling dice by using the Distribute randomly block. Now rolling."
2. The contact reaches the Distribute by percentage block, which routes the customer randomly based on a percentage.
   
   Distribute by percentage simulates a dice roll, resulting in a values between 2 to 12 with different percentages. For example, there is 3 percent chance for the “2” option, 6 percent chance for the “3” option, and so on.
3. After the contact gets routed, the Play prompt tells the customer which number the dice rolled.
4. At the end of the sample, the Transfer to flow block transfers the customer back to the Sample Inbound Flow (p. 53).

**Sample Customer Queue Priority**

Type: Contact flow (inbound)

This sample flow is available in legacy Amazon Connect instances. In new instances, you can see this functionality in Sample Queue Configurations (p. 55).

This contact flow shows you two options for using the Change routing priority/age block to adjust the priority of a customer in the queue. You can change a customer's priority in the queue using priority or routing age.

**Option 1: Raise the Priority**

If the customer presses 1 in the Get Customer Input block, the following Change routing priority/age block changes the Queue priority value of the contact to 1.

By default the priority for new contacts is 5. Lower values raise the priority of the contact. A contact assigned a priority of 1 is routed first.

**Option 2: Change the Routing Age**

If the customer presses 2 in the Get Customer Input block, the following Change routing priority/age block changes the routing age of the contact by increasing the routing age by 10 minutes.

This change prioritizes the contact. Because customers who have been queued longer are connected first, given that the contacts have the same queue priority value.
Sample Disconnect Flow

Type: Contact flow (inbound)

This contact flow only works for chat conversations.

1. The **Play prompt** block shows a text message that the agent has disconnected.
2. A **Wait** block sets the timeout period for 15 minutes. If the customer returns in 15 minutes, the customer is transferred to a queue to chat with another agent.
3. If the customer doesn't return, the timer expires and the chat disconnects.

Sample Queue Customer

Type: Contact flow (inbound)

This contact flow performs checks before placing customer into a queue. Here's how it works:

1. The **Set working queue** block determines which queue to transfer the customer to.
2. The **Check hours of operation** block perform checks to avoid the customer being queued during non-working hours.
3. The customer is transferred to the queue if it is within business hours, and the queue can handle this call. Otherwise, the customer is played a message "We are not able to take your call right now. Goodbye." And then the customer is disconnected.

Sample Queued Callback

Type: Contact flow (inbound)

This sample flow is available in legacy Amazon Connect instances. In new instances, you can see this functionality in Sample Queue Configurations (p. 55).

This contact flow provides callback queue logic. Here's how it works:

1. After a voice prompt, a working queue is selected and its queue status is checked.
2. A voice prompt tells the customer if the wait time for the selected queue is longer than 5 minutes. Customers are offered a choice to wait in the queue or to be placed into a callback queue.
3. If the customer decides to wait in the queue, the **Set customer queue flow** block places them in a queue flow that provides a callback option. That is, it places them in **Sample interruptible queue flow with callback**.
4. If the customer chooses to be placed into a callback queue, their number is stored in the **Store customer input** block. Then their callback number is set, and they are transferred to the callback queue.

Sample Queue Configurations

Type: Contact flow (inbound)

This contact flow shows different ways you can put a customer in queue: you can change the priority of the customer, determine the wait time in queue, and give them an option for a callback. Here's how it works:
1. The customer is put in a basic queue.
2. After that, the Default customer queue flow is invoked.
3. The hours of operation are checked.
4. The channel is checked:
   - If chat, we check the time in queue. If it's less than 5 minutes, the customer is placed in queue for an agent. If it's more, we check the channel again and if it's chat, put the customer in queue for an agent.
   - If voice, we give the customer the option to press 1 to move to the front of the queue or 2 to move to the end of the queue. This is so you can see how to use the Change routing priority / age block to move a contact to the front or back.
5. Next, we check the time in queue again, and then check the channel. If the customer is using voice, we use the Get customer input block to ask if they want a callback or wait in queue.
6. We use a Store customer input block to get the customer's phone number, and a Set callback number block to store it.

Sample Interruptible Queue Flow with Callback

Type: Customer queue

This contact flow shows you how to manage what the customer experiences while in queue. It uses Check contact attributes to determine if the customer is contacting you by phone or chat, and to route them accordingly.

If the channel is chat, the customer is transferred to the Loop prompts.

If the channel is voice, the customer hears a looping audio that interrupts every 30 seconds to give them two options from the Get customer input block:

1. The customer can press 1 to enter a callback number. Then the Get customer input block prompts the customer for their phone number. Then the flow ends.
2. Press 2 ends the flow, and the customer remains in the queue.

Sample Lambda Integration

Type: Contact flow (inbound)

This contact flow shows you how to invoke a Lambda function and do a data dip, that is, retrieve information about the customer. The data dip uses the caller's phone number to look up the US state they are calling from. If the customer is using chat, it returns a fun fact. Here's how it works:

1. A prompt tells the customer that a data dip is being performed.
2. The Invoke Lambda function block triggers sampleLambdaFlowFunction. This sample Lambda function determines the location of the phone number. The function times out in 4 seconds. If it times out, it plays a prompt that says “Sorry, we failed to find the state for your phone number's area code.”
3. In the first Check contact attributes block, it checks the channel the customer is using: voice or chat. If chat, it returns a fun fact.
4. If voice, the second Check contact attributes block is triggered. It checks the match conditions of State, which is an external attribute. It uses an external contact attribute because it's getting data by using a process that's external to Amazon Connect
5. A prompt tells you that it's returning you back to **Sample inbound flow**, and then starts the **Transfer flow** block.
6. If the transfer fails, it plays a prompt and then disconnects the contact.

For more information about using attributes, see Using Attributes with a Lambda Function (p. 88).

**Sample Recording Behavior**

Type: Contact flow (inbound)

This contact flow shows how you can change recording behavior based on user input. It also shows that you can:

- Configure the recording for the agent only.
- Configure the recording for the customer only.
- Configure the recording for both the customer and agent.
- Choose to not have a recording.

It starts by checking the channel of the customer. If the customer is using chat, they get a prompt that the **Set recording block** doesn't apply to chats. Learn more (p. 69).

If the contact is using voice, a **Get customer input** block prompts them to enter the number for who they want to record. Their entry triggers the **Set recording behavior** block with the appropriate configuration.

It ends with the customer being transferred by to the **Sample Inbound Flow** (p. 53).

**Sample Note for Screenpop**

Type: Contact flow (inbound)

This contact flow shows you how to use Screenpop, a Contact Control Panel feature, to load a web page with parameters based on attributes.

In this sample flow, a **Set contact attributes** block is used to create an attribute from a text string. As an attribute, the text can be passed to the CCP to display a note to an agent.

**Sample Secure Input with Agent**

Type: Queue transfer

This contact flow shows you how to allow customers to input sensitive data while putting the agent on hold. In a production environment, we recommend using encryption (p. 121) instead of this solution.

Here's how it works:

1. This flow begins with checking the customer's channel. If they are using chat, they are put in a queue.
2. If they are using voice, the agent and customer are put in a conference call.
3. A **Play prompt** tells the customer that the agent will be put on hold while customer enters their credit card information.
4. When the prompt is finished playing, the agent is put on hold using a **Hold customer and agent** block. If an error occurs, a prompt is played that agent was unable to put on hold, after which the contact flow is ended.
5. The customer's input is stored using the **Store Customer Input** block. This block encrypts the sensitive customer information using a signing key that must be uploaded in .pem format. For a detailed walkthrough that explains how to encrypt customer input, see [Creating a secure IVR solution with Amazon Connect](#).

6. After the customer's data is collected, the agent and customer are put back on call using the **Conference All** option in another **Hold customer and agent** block.

7. The error branch runs if there's an error while capturing the customer's data.

---

**Sample Secure Input with No Agent**

Type: Contact flow (inbound)

This contact flow shows you how to capture sensitive customer data and encrypt it using a key. Here's how it works:

1. It begins by checking the contact's channel. If they are using chat, a prompt is played that this doesn't work with chat, and they are transferred to **Sample Inbound Flow** (p. 53).

2. If they are using voice, the **Store customer input** block prompts them to enter their credit card number. The block stores and also encrypts the data using a signing key that must be uploaded in a .pem format.

   In the **Set contact attributes** block, the encrypted card number is set as contact attribute.

3. After the card number is successfully set as contact attribute, the customer is transferred back to the **Sample Inbound Flow** (p. 53).

---

**Create a New Contact Flow**

The starting point for creating all contact flows is the contact flow designer. It's a drag-and-drop work surface that enables you to link together blocks of actions. For example, when a customer first enters your contact center, you can ask for some input and then play a prompt such as “Thank you.”

For descriptions of the available action blocks, see [Contact Block Definitions](#) (p. 72).

**Before You Begin: Develop a Naming Convention**

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

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

**Choose a Contact Flow Template**

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

When you create a contact flow, you need to choose the right template for your scenario. The following contact flow templates are available.
<table>
<thead>
<tr>
<th>Template</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer queue flow</td>
<td>Use to manage what the customer experiences while in queue, before being joined to an agent. Customer queue flows are interruptible and can include actions such as an audio clip apologizing for a delay and offering an option to receive a callback, leveraging the <code>Transfer to queue</code> block.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice and chat.</td>
</tr>
<tr>
<td>Customer hold flow</td>
<td>Use to manage what the customer experiences while the customer is on hold. With this flow, one or more audio prompts can be played to a customer using the <code>Loop prompts</code> block while waiting on hold.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice.</td>
</tr>
<tr>
<td>Customer whisper flow</td>
<td>Use to manage what the customer experiences as part of an inbound call immediately before being joined with an agent. The agent and customer whispers are played to completion, then the two are joined.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice.</td>
</tr>
<tr>
<td>Outbound whisper flow</td>
<td>Use to manage what the customer experiences as part of an outbound call before being connected with an agent. In this flow, the customer whisper is played to completion, then the two are joined.  For example, this flow can be used to enable call recordings for outbound calls with the <code>Set recording behavior</code> block.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice.</td>
</tr>
<tr>
<td>Agent hold flow</td>
<td>Use to manage what the agent experiences when on hold with a customer. With this flow, one or more audio prompts can be played to an agent using the <code>Loop prompts</code> block while the customer is on hold.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice.</td>
</tr>
<tr>
<td>Agent whisper flow</td>
<td>Use to manage what the agent experiences as part of an inbound call immediately before being joined with a customer. The agent and customer whispers are played to completion, then the two are joined.</td>
</tr>
<tr>
<td></td>
<td>This contact follow works with voice.</td>
</tr>
<tr>
<td>Transfer to agent flow</td>
<td>Use to manage what the agent experiences when transferring to another agent. This type of flow is associated with transfer to agent quick connects, and often plays messaging, then completes the transfer using the <code>Transfer to agent</code> block.</td>
</tr>
</tbody>
</table>
Create a Contact Flow (Inbound)

1. In the navigation pane, choose Routing, Contact flows.
2. Choose Create contact flow. This opens the contact flow designer.
3. Type a name and a description for your contact flow.
4. Search for a contact block using the Search bar, or expand the relevant group to locate the block. For descriptions of the contact blocks, see Contact Block Definitions (p. 72).
5. Drag and drop contact blocks onto the canvas. You can add blocks in any order or sequence, as connections between elements aren't required to be strictly linear.
6. Double-click the title of the block. In the configuration pane, configure settings for that block and then choose Save to close the pane.
7. Back on the canvas, click on the first (the originating) block.
8. Choose the circle for the action to perform, such as Success.
9. Drag the arrow to the connector of the group that performs the next action. For groups that support multiple branches, drag the connector to the appropriate action.
10. Repeat the steps to create a contact flow that meets your requirements.
11. Choose Save to save a draft of the flow. Choose Publish to activate the flow immediately.

Note
All connectors must be connected to a block in order to successfully publish your contact flow.

Generate Logs

After your contact flow is published live, you can use contact flow logs to help analyze contact flows and quickly find errors your customers encounter. If needed, you can roll back to a previous version of the contact flow.
For more information about enabling and using contact flow logs, see Contact Flow Logs (p. 163).

Roll back a Contact Flow

1. In the contact flow designer, open the contact flow you want to roll back.
2. Use the drop-down to choose the version of the contact flow you want to roll back to. If you choose Latest, it reverts the flow to the most recent published version. If there isn’t a published version, it reverts to the most recent saved version.

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

3. Choose Publish to push that version into production.

Associate a Phone Number with a Contact Flow

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

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

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Routing, Phone numbers.
3. You can search for a specific number, filter your search by queue, or select a number from the list provided (if applicable).
4. Select the number to edit, expand Contact flow / IVR, and select the contact flow.
5. Choose Save.

Create Prompts

Prompts are audio files played in call flows. For example, hold music is a prompt. Amazon Connect comes with a set of prompts that you can add to your contact flows. Or, you can add your own recordings.

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.

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

**To create a prompt**

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

**Tip**

If you enter text that isn't supported for the Amazon Polly voice you are using, it won't be played. However, any other supported text in the prompt will be played. For a list of supported languages, see Languages Supported by Amazon Polly.

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.

**Use SSML Tags to Personalize Text-to-Speech**

When you add a prompt to a contact flow, you can use SSML tags to provide a more personalized experience for your customers. SSML tags are a way to control how Amazon Polly generates speech from the text you provide. To learn more about the SSML tags, see SSML Tags Supported by Amazon Polly.

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.

Amazon Connect supports the following SSML tags. To learn how to use these tags together to achieve a natural sounding voice, see SSML in Amazon Connect Contact Flows.
### Set Up Contact Transfers

To make it easy for you to set up contact transfers, Amazon Connect provides you with several tools:

- **Two contact flow types:**
  - **Transfer to agent:** Enables transfers to another agent. This works with voice contacts.
  - **Transfer to queue:** Enables transfers to a queue. This works with both voice and chat contacts.
- **Action blocks:**
  - **Transfer to queue:** Use to end the current contact flow and place the customer in a queue. This block works for both voice and chat transfers.
  - **Transfer to phone number:** Use to transfer the customer to a phone number, such as an external number. This block works for voice transfers.
  - **Transfer to flow:** Use to end the current flow and transfer the customer to another contact flow. This block works for voice transfers.
- **Quick connects:** Use to create common destinations for transfers. Agents will see them as options in the CCP when they go to do a transfer.

If you use an unsupported tag in your input text it is automatically ignored when it is processed.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Use to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>speak</td>
<td>All SSML-enhanced text must be enclosed within a pair of speak tags.</td>
</tr>
<tr>
<td>break</td>
<td>Add a pause to your text. The maximum duration for a pause is 10 seconds.</td>
</tr>
<tr>
<td>lang</td>
<td>Specify another language for specific words.</td>
</tr>
<tr>
<td>mark</td>
<td>Put a custom tag within the text.</td>
</tr>
<tr>
<td>p</td>
<td>Add a pause between paragraphs in your text.</td>
</tr>
<tr>
<td>phoneme</td>
<td>Make a phonetic pronunciation for specific text.</td>
</tr>
<tr>
<td>prosody</td>
<td>Control the volume, rate, or pitch of your selected voice.</td>
</tr>
<tr>
<td>s</td>
<td>Add a pause between lines or sentences in your text.</td>
</tr>
<tr>
<td>say-as</td>
<td>Combine with the interpret-as attribute to tell Amazon Polly how to say certain characters, words, and numbers.</td>
</tr>
<tr>
<td>sub</td>
<td>Combine with the alias attribute to substitute a different word (or pronunciation) for selected text such as an acronym or abbreviation.</td>
</tr>
<tr>
<td>w</td>
<td>Customize the pronunciation of words by specifying the word’s part of speech or alternate meaning.</td>
</tr>
<tr>
<td>amazon:effect name=&quot;whispered&quot;</td>
<td>Indicate that the input text should be spoken in a whispered voice rather than as normal speech.</td>
</tr>
</tbody>
</table>
Overview of Steps

To set up call transfers and quick connects

1. Choose a contact flow type based on what you want to do: Transfer to agent or Transfer to queue. External transfers do not require a specific type of contact flow.
2. Create and publish the contact flow.
3. Create a quick connect for the type of transfer to enable: Agent, Queue, or External.

   When you create the Agent or Queue quick connect, select a contact flow that matches the type of transfer to enable. External quick connects require only a phone number, and do not allow you to set a queue or contact flow.
4. Add the quick connect that you created to any queue used in a contact flow for which to enable contact transfer, such as the queue used in the contact flow for incoming contacts. Make sure the queue is in a routing profile assigned to the agents who transfers contacts.

Create Quick Connects

Quick connects are a way for you to create a list of destinations for common transfers. For example, you might create a quick connect for Tier 2 support. If agents in Tier 1 support can't solve the issue, they will transfer the contact to Tier 2.

When you create a quick connect, you can specify one of these destinations:

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

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

To create a quick connect

1. Choose Routing, Quick connects, Add a new destination.
2. Enter a name for the connect. Choose the type, and then specify the destination (such as a phone number or the name of an agent), contact flow (if applicable), and description.

   **Important**
   A description is required when you create a quick connect. If you don't add one, you'll get an error when you try to save the quick connect.
3. To add more quick connects, choose Add new.
4. Choose Save.

To enable your agents to see the quick connects in the CCP when they transfer a contact

1. After you create the quick connect, go to Routing, Queues and then choose the appropriate queue for the contact to be routed to.
2. On the Edit queue page, in the Quick connect box, search for the quick connect you created.
3. Select the quick connect and then choose Save.
Resume a Contact Flow After Transfer

Let's say you need to transfer a contact to an external department that's not using Amazon Connect. For example, maybe you need to transfer the caller to a shipping provider to check the status of their delivery. After the contact is disconnected from the external number, you want them to be returned to your agent, for example, when the delivery company couldn't resolve their issue.

- For advanced automation, send tracking information as DTMF digits when the call is transferred, so that the shipment information is retrieved with the transferred call before the customer is connected.

To set up a contact flow for this scenario

1. Add a Transfer to phone number block to your contact flow.
2. In the Transfer to phone number block, enter the following settings:
   - Transfer to
     - Phone number—Sets the phone number to transfer the call to.
     - Use attribute—Specify a contact attribute to set the phone number to transfer the call to.
   - Set timeout
     - Timeout (in seconds)—The number of seconds to wait for the recipient to answer the transferred call.
   - Use attribute—Specify a contact attribute to use to set the Timeout duration.
   - Resume contact flow after disconnect—When you select this option, after the call is transferred, the caller is returned to the contact flow when the call with the third party ends. Additional branches for Success, Call failed, and Timeout are added to the block when you select this option so that you can appropriately route contacts when there is an issue with the transfer.
   - Optional parameters
     - Send DTMF—Select Send DTMF to include up to 50 Dual-Tone Multi-frequency (DTMF) characters with the transferred call. You can enter the characters to include, or use an attribute. Use the DTMF characters to navigate an automated IVR system that answers the call.
     - Caller ID number—Specify the caller ID number used for transferred call. You can select a number from your instance, or use an attribute to set the number.
     - Caller ID name—Specify the caller ID name used for the transferred call. You can enter a name, or use an attribute to set the name.

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

When the block executes:

1. The call is transferred to the external number.
2. Optionally, when the conversation with the external party ends, the contact is returned to the contact flow.
3. The contact then follows the Success branch from the block to continue the flow.
4. If the call is not successfully transferred, one of the other branches is followed: Call failed, Timeout, or Error, depending on the reason the caller did not return to the flow.
Manage Contact in a Queue Using a Transfer to Queue Block

For inbound contacts, you can define advanced routing decisions to minimize queue wait times, or route contacts to specific queues, using blocks in your contact flow. For example, use a Check queue status block to check staffing or agent availability for a queue before sending a contact to that queue, or use a Get queue metrics block to retrieve queue metrics. Then use a Check contact attributes block to check specific queue metric attributes, and define conditions in the block to determine which queue to route the contact to based on attribute values. For more information about using queue metrics, see How to Use System Metric Attributes (p. 93).

After determining which queue to transfer the contact to, use a Transfer to queue block in a contact flow to transfer the contact to that queue. When the Transfer to queue block runs, it checks the queue capacity to determine whether or not the queue is at capacity (full). This check for queue capacity compares the current number of contacts in the queue to the Maximum contacts in queue limit, if one is set for the queue. If no limit is set, the queue is limited to the number of concurrent active contacts set in the service limit for the instance.

After the contact is placed in a queue, the contact remains there until an agent takes the contact, or until the contact is handled based on the routing decisions in your customer queue flow. To change the queue associated with the call after it is already placed in a queue, use a Loop prompts block with a Transfer to queue block in a customer queue flow. In the block choose which queue to transfer the call to, or use an attribute to set the queue.

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 contacts in a queue using a Transfer to queue block

1. In Amazon Connect, choose Routing, Contact flows.
2. Choose the down arrow next to Create contact flow, then choose Create customer queue flow.
3. Under Interact, add a Loop prompts block to provide a message to the caller when the call is transferred, then every X seconds or minutes while the call is in the queue.
4. Select the Loop prompts block to display the settings for the block.
5. Choose Add another prompt to the loop.
6. Under Prompts, do one of the following:
   - Choose Audio recording in the drop-down menu, then select the audio recording to use as the prompt.
   - Choose Text to Speech in the drop-down menu, then enter text to use for the prompt in the Enter text to be spoken field.
7. To set an interrupt, choose Interrupt every, enter a value for the interrupt interval, and then choose a unit, either Minutes or Seconds. We recommend that you use an interval greater than 20 seconds to ensure that queued contacts that are being connected to an agent are not interrupted.
8. Choose Save.
9. Connect the block to the Entry point block in the contact flow.
10. Under Terminate/Transfer, drag a Transfer to queue block onto the designer.
11. Select the title of the block to display the settings for the block, then choose the Transfer to queue tab.
12. Under Queue to check, choose Select a queue, then select the queue to transfer calls to.
Alternatively, choose **Use attribute**, then reference an attribute to specify the queue. If you use an attribute to set the queue, the value must be the queue ARN.

13. Choose **Save**.
14. Connect the **Loop prompt** block to the **Transfer to queue** block.
15. Add additional blocks to complete the contact flow that you require, such as the blocks to check queue status or metrics, then choose **Save**.

The contact flow is not active until you publish it.

**Important**
To successfully complete the call transfer to another queue, you must include a block after the **Transfer to queue** block and connect the **Success** branch to it. For example, use an **End flow / Resume** block to end the contact flow. The flow does not end until the call is picked up by an agent.

### Transfer Contacts Directly to a Specific Agent

With agent queues, you can route contacts directly to a specific agent. This allows you to provide a consistent customer experience for your customers by letting you route contacts 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 who are assigned permissions to use the Contact Control Panel (CCP) can use the CCP to receive contacts. The Agent and Admin security profiles are the only default security profiles that include permissions to use the CCP. If you route a contact to someone who doesn't have these permissions, the contact can never be handled.

**To route a contact directly to a specific agent**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. In the contact flow designer, open an existing contact flow, or create a new one.
3. Add a block in which you can select a queue to transfer a contact to, such as a **Set working queue** block.
4. Select the title of the block to open the block settings.
5. Select **By agent**.
6. Under **Select an agent**, enter the user name of the agent, or select the agent's user name from the drop-down list.
7. Choose **Save**.
8. Connect the **Success** branch to the next block in your contact flow.

You can also choose to use an attribute to select the queue created for the agent user account. To do so, after you choose **By agent**, choose **Use attribute**.
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 (p. 150). The agent events, which are included in the agent event data stream, include the agent ARN. The user ID is included in the agent ARN after `agent/`.

In the following agent event data, the agent ID is **87654321-4321-4321-123456789012**.

```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"
        }],
        "Name": "Basic Routing Profile"
      },
      "Username": "agentUserName"
    },
    "Contacts": []
  }
}
```
Set Up Recording Behavior

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

A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the flow.

Agents and contacts are stored on separate, stereo audio channels.

- The agent audio is stored in the right channel.
- All incoming audio, including the customer and anyone conferenced in, is stored in the left channel.

Recordings are stored in the Amazon S3 bucket that you specify for your instance (p. 30). This allows access by any user or application with the appropriate permissions. Encryption is enabled by default for all call recordings using Amazon S3 server-side encryption with KMS. You shouldn't disable encryption.

**Important**
For voice conversations, you enable recording in the contact flow block, and you can specify whether to record the agent, customer, or both. For chat conversations, you enable recording at the instance level. If there's an S3 bucket for storing chat transcripts, then all chats are recorded. If no bucket exists, then no chats are recorded.

**To set up recording behavior in your contact flows**

1. Log in to your Amazon Connect instance using an account that has permissions to edit contact flows.
2. Choose Routing, Contact flows, and then open the contact flow that handles customer contacts you want to monitor.
3. Before the contact is connected to an agent, add a Set recording 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. Open Set recording behavior to configure it. Choose what you want to record: Agent, Chat bot, Customer, or all of them.
5. To enable manager monitoring and recording for outbound calls, the contact flow in which you add Set recording behavior must be in the flow selected as the outbound contact flow for the queue used for outbound calls.
6. 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 set up recording behavior for outbound calls**

1. Create a contact flow, using the outbound whisper flow type.
2. Add Set recording behavior to that contact flow.
3. Set up a queue that will be used for making outbound calls. In the Outlook whisper flow box, choose the contact flow that has Set recording behavior in it.

To learn what permissions managers need so they can monitor live conversations and review recordings of past conversations, see Review Recorded Conversations (p. 144).
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.

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

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

**About Using Dynamic Caller ID**

If you use an attribute to set the caller ID number dynamically, the attribute can be one you define in the **Set contact attributes** block in the contact flow. Or, it can be an external attribute returned from an AWS Lambda function.

The value of the attribute must be a phone number from your instance in E.164 format.

- If the number is not in E.164 format, the number from the queue associated with the outbound whisper flow is used for the caller ID number.
- If no number is set for the outbound caller ID number for the queue, the call attempt will fail.

For more information about E.164, see [Use E.164 Format for Telephone Numbers (p. 48)](https://docs.aws.amazon.com/connect/latest.AdminGuide/ dubbed_data_types.html).

**How Caller ID Works in Call phone number Block**

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

- The caller ID number is set if one is specified in the **Call phone number** block.
- If no caller ID is specified in the **Call phone number** block, the caller ID number defined for the queue is used when the call is placed.
- When there is an error with a call that is initiated by the **Call phone number** block, the call is disconnected and the agent is placed in ACW status.

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

**Specify a Custom Caller ID Number Using a Call phone number Block**

1. In Amazon Connect choose **Routing, Contact flows**.
2. Choose the down arrow next to **Create contact flow**, and then choose **Create outbound whisper flow**.
3. Add a **Call phone number** block to the flow, and connect the **Entry point** block to it.
   - The **Call phone number** block must be placed before a **Play prompt** block if one is included in your contact flow.
4. Select the **Call phone number** block, and then select **Caller ID number to display**.
5. Do one of the following:
To use a number from your instance, choose **Select a number from your instance**, and then search for or select the number to use from the drop-down.

Choose **Use attribute** to use a contact attribute to provide the value for the caller ID number. You can use either a **User Defined** attribute you create using a **Set contact attributes** block, or an **External** attribute returned from an AWS Lambda function. The value of any attribute you use must be a phone number claimed for your instance and be in E.164 format. If the number used from an attribute is not in E.164 format, the number set for the **Outbound caller ID number** for the queue is used.

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

---

## Import/Export Contact Flows

You can export contact flows from and import contact flows into your Amazon Connect instance. This lets you 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 designer 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.

## Resolve Resources in Imported Contact Flows

When you create a contact flow, the resources you include in the contact flow, such as queues and voice prompts, are referenced within the contact flow using the name of the resource and the Amazon Resource Name (ARN). The ARN is a unique identifier for a resource that is specific to the service and Region in which the resource is created. When you export a contact flow, the name and ARN for each resource referenced in the contact flow is included in the exported contact flow.

When you import a contact flow, Amazon Connect attempts to resolve the references to the Amazon Connect resources used in the contact flow, such as queues, by using the ARN for the resource. When you import a contact flow into the same Amazon Connect instance that you exported it from, the resources used in the contact flow will resolve to the existing resources in that instance. If you delete a resource, or change the permissions for a resource, Amazon Connect may not be able to resolve the resource when you import the contact flow. When a resource cannot be found using the ARN, Amazon Connect attempts to resolve the resource by finding a resource with the same name as the one used in the contact flow. If no resource with the same name is found, a warning is displayed on the block that contains a reference to the unresolved resource.

If you import a contact flow into a different Amazon Connect instance than the one it was exported from, the ARNs for the resources used are different. If you create resources in the instance with the
same name as the resource in the instance where the contact flow was exported from, the resources can be resolved by name. You can also open the blocks that contain unresolved resources, or resources that were resolved by name, and change the resource to another one in the Amazon Connect instance. You can save a contact flow with unresolved or missing resources, but you cannot publish it until the resources are resolved or removed.

Export and Import a Contact Flow

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**. When the contact flow is imported into an existing contact flow, the name of the existing contact flow is updated, too.
6. Review and update any resolved or unresolved references as necessary.
7. To save the imported flow, choose **Save**. To publish, choose **Save and Publish**.

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 canvas.

This topic describes all of the available action blocks.
**Note**
When you set User Defined or External values in dynamic attribute fields, use only alphanumeric characters (A-Z, 0–9) and periods. No other characters are allowed.

**Interact Blocks**

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play prompt</td>
<td>Plays an interruptible audio prompt, delivers a text-to-speech message, or delivers a chat response.</td>
<td>When you use text (for text-to-speech or chat) you can use a maximum of 3,000 billed characters (6,000 total characters). You can also specify text in a flow using a contact attribute. To learn how to record and upload an audio file, and add text-to-speech, see Create Prompts (p. 61).</td>
</tr>
<tr>
<td>Get customer input</td>
<td>Branches based on customer intent.</td>
<td>This action block includes the Play prompt in it: it plays an interruptible audio prompt, text-to-speech, or a chat message for a customer to respond to. It then branches based on the customer's input. The input can be DTMF, a chat response, or an Amazon Lex intent. A sample configuration is shown in the following image.</td>
</tr>
</tbody>
</table>

When you use text (for text-to-speech or chat) you can use a maximum of 3,000 billed characters (6,000 total characters).

Amazon Lex bots support both spoken utterances and keypad input when used in a contact flow.
### Interact Blocks

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tip</strong></td>
<td></td>
<td>You can prompt contacts to end their input with a pound key # and to cancel it using the star key *.</td>
</tr>
<tr>
<td><strong>Store customer input</strong></td>
<td>Stores numerical input to contact attribute.</td>
<td>This action block is similar to Get customer input, only this one stores the input as a contact attribute and allows you to encrypt it. This way you can encrypt sensitive input such as credit card numbers. It includes the Play prompt. It plays an interruptible audio prompt, text-to-speech, or a chat message for a customer to respond to. You can specify the amount of time to wait for a customer to enter their reply by voice or chat, and whether to encrypt their reply. For detailed information about how to encrypt customer input, see Creating a secure IVR solution with Amazon Connect.</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Loop prompts          | Loops a sequence of prompts while a customer or agent is on hold or in queue. | When **Loop prompts** is used in a queue flow, audio playback can be interrupted with a flow at preset times.  

**Tip**  
Always use an interruption period that's greater than 20 seconds. This is the amount of time an available agent has to accept the contact.  
If the interruption period is less than 20 seconds, you might get contacts going down the Error branch. This is because Amazon Connect doesn't support dequeueing the customer when they are being routed to an active agent and are in the 20 second window to join.  
If this block is triggered during a chat conversation, the contact is routed down the Error branch.  

**Tip**  
Some existing contact flows have a version of the **Loop prompts** block that doesn't have an error branch. In this case, a chat contact stops execution of the customer queue flow. The chat is routed when the next agent becomes available.  

| Hold customer or agent | Places a customer or agent on or off hold.       | Settings:  
Agent on hold / customer on call  
Customer on hold / agent on call  
Agent and customer on call  
If this block is triggered during a chat conversation, the contact is routed down the Error branch. |
## Set Blocks

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call phone number</td>
<td>Initiates an outbound call from</td>
<td>Use the <strong>Call phone number</strong> 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></td>
<td>an outbound whisper flow.</td>
<td></td>
</tr>
<tr>
<td>Start media streaming</td>
<td>Starts capturing customer audio for</td>
<td>Captures customer audio during a contact. You must enable Live media streaming to successfully capture customer audio. Media streaming continues until a <strong>Stop media streaming</strong> block is used or the contact ends. To learn more, see Capture Customer Audio: Live Media Streaming (p. 122).</td>
</tr>
<tr>
<td></td>
<td>a contact.</td>
<td></td>
</tr>
<tr>
<td>Stop media streaming</td>
<td>Stops capturing customer audio after</td>
<td>After it's started, media streaming continues, even when one contact flow transfer to another contact flow. You must use a <strong>Stop media streaming</strong> block to stop media streaming.</td>
</tr>
<tr>
<td></td>
<td>it is started with a **Start media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>streaming** block.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this block is triggered during a chat conversation, the contact is routed down the Error branch.</td>
</tr>
</tbody>
</table>

### Set Blocks

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set working queue</td>
<td>Specifies the queue to be used when **Transfer</td>
<td>A queue must be specified before invoking <strong>Transfer to queue</strong> 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>to queue** is invoked.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To use a <strong>Set working queue</strong> block to set the queue dynamically, such as with</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set recording behavior</td>
<td>Sets options for recording conversations.</td>
<td>Enables or disables recording of the agent, chat bot, customer, or all three.________________________________________________________________________________________________________________________________</td>
</tr>
<tr>
<td>Set contact attributes</td>
<td>Stores key-value pairs as contact attributes.</td>
<td>Contact attributes are accessible by other areas of Amazon Connect, such as the CTRs. For more information about how to use contact attributes, see Use Amazon Connect Contact Attributes (p. 84).</td>
</tr>
<tr>
<td>Get queue metrics</td>
<td>Retrieves real-time metrics about queues and agents in your contact center and returns them as attributes.</td>
<td>Use a Check contact attributes 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 How to Use System Metric Attributes (p. 93).</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Change routing priority / age</strong></td>
<td>Changes the priority of the contact in queue. You may want to do this, for example, based on the contact's issue or other variable.</td>
<td>This block gives you two options for changing a contact's position in queue:&lt;br&gt;• <strong>Set priority.</strong> The default priority for new contacts is 5. You can raise the priority of a contact - compared to other contacts in the queue - by assigning them a higher priority, such as 1 or 2.&lt;br&gt;• <strong>Adjust by time.</strong> You can add or subtract seconds or minutes from the amount of time the contact spends in queue. Since contacts are routed to agents on a first-come first-served basis, changing their amount of time in queue compared to others also changes their position in queue.&lt;br&gt;“Time in queue” is the amount of time the contact spends in queue before they are routed to an agent or removed from the queue.) For example, you can add or subtract seconds or minutes.&lt;br&gt;To view a sample flow that uses this block, see Sample Queue Configurations (p. 55).</td>
</tr>
<tr>
<td><strong>Set hold flow</strong></td>
<td>Links from one contact flow type to another.</td>
<td>Specifies the flow to invoke when a customer or agent is put on hold.&lt;br&gt;If this block is triggered during a chat conversation, the contact is routed down the Error branch.</td>
</tr>
<tr>
<td><strong>Set whisper flow</strong></td>
<td>Overrides the default whisper by linking to a whisper flow.</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>
</tbody>
</table>
### Branch Blocks

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
<tr>
<td>Set disconnect flow</td>
<td>Sets the flow to run when the agent disconnects from the chat.</td>
<td>An example of when you would use Set disconnect flow is when a customer stops responding to the chat. Use this block to decide whether to run the disconnect flow and call a Wait block, or end the conversation.</td>
</tr>
</tbody>
</table>

### Branch Blocks

<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</td>
<td>Branches based on whether agents are available, staffed.</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>are available, staffed (on call, or after contact work status), or online.</td>
<td>(available, on call, and after contact work), or online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must set a queue before using a <strong>Check staffing</strong> block in your contact flow. If a queue is not set, the 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 occurring within or outside of the hours of operation defined for the queue.</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></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>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 percentage.</td>
<td>Like flipping a coin, contacts are distributed randomly, which doesn't guarantee exact percentage splits.</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Loop</td>
<td>Loops through (repeats) the <strong>Looping</strong> branch for the number of loops specified.</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. 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 Block

<table>
<thead>
<tr>
<th>Block</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Pauses the contact flow.</td>
<td>Use this block in chat contact flows only. If a contact stops responding to a chat, this block pauses the contact flow for the specified wait time. It has two branches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Timeout: Run this branch if the customer hasn't sent a message after a specified amount of time. Maximum is 24 hours.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer return: Run this branch when the customer returns and sends a message. With this branch you can route the customer to the previous (same) agent, previous (same) queue, or override and set a new working queue/agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this block is started during a voice conversation, the contact is routed down the Error branch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can add multiple <strong>Wait</strong> blocks to your contact flows. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the customer comes back in 5 minutes, connect them to the same agent. This is because that agent has all of the context.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the customer doesn’t come back after 5 minutes, send a text saying &quot;We missed you.&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the customer comes back in 12 hours, connect to a contact flow that puts them in a priority queue. However, it doesn't route them to the same agent.</td>
</tr>
</tbody>
</table>

### Integrate Block

<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.</td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Terminate / Transfer Blocks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>Disconnect / hang up</td>
<td>Terminates a customer contact.</td>
<td>Disconnects the customer.</td>
</tr>
<tr>
<td>Transfer to queue</td>
<td>In most contact flows, this block ends the current contact flow and places the customer in queue. When used in a customer queue flow, this block transfers a contact already in a queue to another queue.</td>
<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>Transfer to phone number</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 resumes the contact flow after the transferred call ends. If the country you want to select is not listed, you can submit a request to add countries you want to transfer calls to using the Amazon Connect service limits increase form.</td>
</tr>
</tbody>
</table>
Use Amazon Connect Contact Attributes

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

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

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

Contents

• Contact Attribute Concepts (p. 85)
Contact Attribute Concepts

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

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

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

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.

### How to Use Contact Attributes to Personalize the Customer Experience

Contact attributes in your contact flows can provide a more personalized customer experience. For example, specify a custom flow based on comparing an attribute to a value. You then route the contact based on the value comparison, such as routing customers to different tiers of support based on their account number. Or retrieve a customer's name and save it as an attribute. Include the name attribute in a text to speech string so that the customer's name is said during the interaction.

**Tip**

Contact attributes are shared across all contacts with the same InitialContactId. This means that while carrying out transfers, for example, a contact attribute updated in the transfer flow updates the attribute's value in both CTR's contact attributes (that is, the Inbound and Transfer contact attributes).

The steps in the following sections describe how to use contact attributes with different blocks in a contact flow.

### Using a Set Contact Attributes Block

Use a **Set contact attributes** block to set a value that is later referenced in a contact flow. For example, create a personalized greeting for customers routed to a queue based on the type of customer account. You could also define an attribute for a company name or line of business to include in the text to speech strings said to a customer. The **Set contact attributes** block is useful for copying attributes retrieved from external sources to user-defined attributes.

**To set a contact attribute with a Set contact attributes block**

1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing contact flow, or create a new one.
3. Add a **Set contact attributes** block.
4. Edit the **Set contact attributes** block, and choose Use text.
5. For the Destination key, provide a name for the attribute, such as Company. This is the value you use for the Attribute field when using or referencing attributes in other blocks. For the Value, use your company name.

You can also choose to use an existing attribute as the basis for creating the new attribute.

### 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 block](image)

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 Contact Attributes for Personalization

Using Attributes with a Lambda Function

Retrieve data from a system your organization uses internally, such as an ordering system or other database with a Lambda function, and store the values as attributes that can then be referenced in a contact flow.

When the Lambda function returns a response from your internal system, the response is key-value pairs of data. You can reference the values returned in the External namespace, for example $.External.attributeName. To use the attributes later in a contact flow, you can copy the key-value pairs to user-defined attributes using a Set contact attributes block. You can then define logic to branch your contact based on attribute values by using a Check contact attributes block. Any contact attribute retrieved from a Lambda function is overwritten with the next invocation of a Lambda function. Make sure you store external attributes if you want to reference them later in a contact flow.

To store an external value from a Lambda function as a contact attribute

1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing contact flow, or create a new one.
3. Add an Invoke AWS Lambda function block, then choose the title of the block to open the settings for the block.
4. Add the Function ARN to your AWS Lambda function that retrieves customer data from your internal system.
5. After the Invoke AWS Lambda function block, add a Set contact attributes block and connect the Success branch of the Invoke AWS Lambda function block to it.
6. Edit the Set contact attributes block, and select Use attribute.
7. For Destination key, type a name to use as a reference to the attribute, such as customerName. This is the value you use in the Attribute field in other blocks to reference this attribute.
8. For the Type, choose External.
9. For **Attribute** type the name of the attribute returned from the Lambda function. The name of the attribute returned from the function will vary depending on your internal system and the function you use.

After this block executes during a contact flow, the value is saved as a user-defined attribute with the name specified by the **Destination key**, in this case customerName. It can be accessed in any block that uses dynamic attributes.

To branch your contact flow based on the value of an external attribute, such as an account number, use a **Check contact attributes** block, and then add a condition to compare the value of the attribute to.

Next, branch the contact flow based on the condition.

1. In the **Check contact attributes** block, for **Attribute to check** do one of the following:
   - Select **External** for the **Type**, then enter the key name returned from the Lambda function in the **Attribute** field.
     
     **Important**
     Any attribute returned from an AWS Lambda function is overwritten with the next function invocation. To reference them later in a contact flow, store them as user-defined attributes.
   - Select **User Defined** for the **Type**, and in the **Attribute** field, type the name that you specified as the **Destination key** in the **Set contact attributes** block.

2. Choose **Add another condition**.

3. Under **Conditions to check**, choose the operator for the condition, then enter a value to compare to the attribute value. A branch is created for each comparison you enter, letting you route the contact based on the conditions specified. If no condition is matched, the contact takes the **No Match** branch from the block.

**"$" is a Special Character**

Amazon Connect treats the "$" character as a special character. You can't use it in a key when setting an attribute.

For example, let's say you're creating an interact block with text-to-speech. You set an attribute like this:

```json
{"$one":"please read this text"
```

When Amazon Connect reads this text, it will read "dollar sign one" to the contact instead of "please read this text." Also, if you were to include $ in a key and try to reference the value later using Amazon Connect, it won't retrieve the value.

Amazon Connect does log and pass the full key:value pair ("$_$one":"please read this text") to integrations such as Lambda.

**Use Amazon Connect Contact Attributes with Other Services**

You can reference contact attributes set in your Amazon Connect contact flow in other services, such as in an Amazon Lex bot or AWS Lambda function. This allows data associated with the customer or the contact to be shared between services. To use contact attributes to access other resources, set a user-defined attribute in your contact flow and use the Amazon Resource Name (ARN) of the resource you want to access as the value for the attribute. For example, to use an Amazon Connect prompt in a
Lambda function, set a user-defined attribute to the ARN for the prompt, and then access that attribute from the Lambda function.

Use Contact Attributes in the CCP

Contact attributes also let you capture information and then present that information in a screenpop to an agent in the Contact Control Panel (CCP). Use contact attributes to customize the agent experience when using the CCP integrated with a customer relationship management (CRM) application. Also use them when integrating Amazon Connect with a custom application using the Amazon Connect Streams API or Amazon Connect API. You can use all user-defined attributes, in addition to the customer number and the dialed number, in the CCP using the Amazon Connect Streams JavaScript library. For more information, see Amazon Connect Streams API or Amazon Connect API.

When you use the Amazon Connect Streams API, you can access user-defined attributes by invoking contact.getAttributes(). You can access endpoints via contact.getConnections(), where a connection has a getEndpoint() invocation on it.

To access the attribute directly from a Lambda function, use $.External.AttributeName. If the attribute is stored to a user-defined attribute from a Set contact attributes block, use $.Attributes.AttributeName.

For example, included with your Amazon Connect instance, there is a contact flow named “Sample note for screenpop.” In this contact flow, a Set contact attributes block is used to create an attribute from a text string. The text, as an attribute, can be passed to the CCP to display a note to an agent.

How to Reference Contact Attributes

The way you reference contact attributes depends on how they were created and how you are accessing them. To reference attributes in the same namespace, such as a system attribute, you use the attribute name, or the name you specified as the Destination key. To reference values in a different namespace, such as referencing an external attribute, you specify the JSONPath syntax to the attribute.

For example, to reference a customer name from a Lambda function lookup, you use $.External.AttributeKey, replacing AttributeKey with the key (or name) of the attribute returned from the Lambda function. To reference an attribute from an Amazon Lex bot, you use the format $.Lex. and then include the part of the Amazon Lex bot to reference, such as $.Lex.IntentName. To reference the customer input to an Amazon Lex bot slot, use $.Lex.Slots.slotName, replacing slotName with the name of the slot in the bot.

To reference user-defined attributes, such as those set with the Set contact attributes block, use the drop-down menus in subsequent blocks to reference the attribute, or use the Attributes namespace in JSONPath to the attribute if used in a text field. For example, if you create a user-defined attribute in a Set contact attributes block, you reference it in one of the following ways:

- In a block that supports attributes, such as a Check contact attributes block, choose User Defined for the Type, and use the value you entered for the Destination key in the Attribute field.
- In a text field in a block, such as a Play prompt block, use the JSONPath $.Attributes.DestinationKey, replacing DestinationKey with the value you entered in the Destination key.

JSONPath is a standardized way to query elements of a JSON object. JSONPath uses path expressions to navigate elements, nested elements, and arrays in a JSON document. For more information about JSON, see Introducing JSON.

Checking Attribute Values in a Check Contact Attributes Block

When you include a Check contact attributes block in a contact flow, it checks the value of the attribute you specify. You then add a condition to compare the value of the attribute to, such as “greater than"
or "contains." For each condition you add, an output branch is added to the block. You can then route the contact based on the conditions by connecting the output branch for the condition to the next block in the contact flow. For example, you can check the current number of customers in a queue, then route the contact to the queue if the active contacts are fewer than 5. You can also route the contact to another different queue if the number of active contacts is more than 5. You can use whichever metrics or attributes you want to make routing decisions as appropriate for your needs. The following procedure describes how to check for the number of contacts in a queue and then route the contact to a queue that has fewer than 5 active contacts in it.

Using a Check contact attributes block to route a contact to a queue

1. In Amazon Connect, choose Routing, Contact flows.
2. Open an existing contact flow or create a new one.
3. Optionally, under Interact, add a Play prompt block to the designer to play a greeting to your customers. Add a connector between the Entry point block and the Play prompt block.
4. Under Set, drag a Get queue metrics block to the designer, and connect the Okay branch of the Play prompt block to it.
5. Choose the title of the Get queue metrics block to open the properties for the block. By default, the block retrieves metrics for the current working queue. To retrieve metrics for a different queue, choose Set queue.
6. Choose Select a queue, then select the queue to retrieve metrics for from the drop-down, then choose Save.

You can also determine which queue to retrieve metrics for using contact attributes.
7. Under Branch, drag a Check contact attributes block to the designer.
8. Choose the title of the block to display the settings for the block. Then, under Attribute to check, select Queue metrics in the Type drop-down menu.
9. Under Attribute, choose Contacts in queue.
10. To use conditions to route the contact, choose Add another condition.

By default, the Check contact attributes block includes a single condition, No match. The No match branch is followed when there are no matches for any of the conditions you define in the block.
11. Under Conditions to check, select Is less than as the operator for the condition in the drop-down menu, then in the value field enter 5.
12. Choose Add another condition, then choose Is greater or equal from the drop-down menu, and enter 5 in the value field.
13. Choose Save.

You now see two new output branches for the Check contact attributes block.

You can now add additional blocks to the contact flow to route the contact as desired. For example, connect the < 5 branch to a Transfer to queue block to transfer calls to the queue when there are fewer than five calls currently in the queue. Connect the > 5 branch to a Set customer callback number block and then transfer the call to a callback queue using a Transfer to queue block so the customer doesn't have to stay on hold.

Referencing Attributes from a Play Prompt Block

Use a Play prompt block to use an audio file to play as a greeting or message to callers. You can also use contact attributes to specify the greeting or message delivered to callers. To use the values of a contact attribute to personalize a message for a customer, include references to stored or external contact attributes in the text-to-speech message. For example, if you retrieved the customer's name from a Lambda function, and it returns values from your customer database for FirstName and LastName, you
could use these attributes to say the customer's name in the text-to-speech block by including text similar to the following:

```
Hello $.External.FirstName $.External.LastName, thank you for calling.
```

Alternatively, you could store the attributes returned from the Lambda function using a **Set contact attributes** block, and then reference the user-defined attribute created in the text to speech string.

---

**Getting Customer Input Using an Amazon Lex Bot**

When you reference attributes in a **Get customer input** block, and choose Amazon Lex as the method of collecting the input, the attribute values are retrieved and stored from the output from the customer interaction with the Amazon Lex bot. You can use an attribute for each intent or slot used in the Amazon Lex bot, as well as the sessions attributes associated with the bot. An output branch is added to the block for each intent you include. When a customer chooses an intent when interacting with the bot, the branch associated with that intent is followed in the contact flow.

**Using an Amazon Lex bot to get customer input**

1. In Amazon Connect, choose **Routing, Contact flows**.
2. Open an existing or create a new contact flow.
3. Under **Interact**, drag a **Get customer input** block to the designer.
4. Choose the title of the block to display the block settings, then select **Text to speech (Ad hoc)**.
5. Choose **Enter text**, then enter text in the **Enter text to be spoken** field that is used as a message or greeting to your customers. For example, "Thank you for calling" followed by a request to enter information to fulfill the intents you defined in your Amazon Lex bot.
6. Choose the **Amazon Lex** tab, then from the drop-down menu, choose the Amazon Lex bot to use to get customer input.
7. By default, the **Alias** field is populated with "$LATEST". To use a different alias of the bot, enter the alias value to use.
8. Optionally, to pass an attribute to Amazon Lex to use as a session attribute, choose **Add an attribute**. Specify the value to pass using either text or an attribute.
9. To create a branch from the block based on the customer intent, choose Add an intent, then enter the name of the intent exactly the same as the intent name in your bot.
10. Choose Save.

How to Use System Metric Attributes

Amazon Connect includes system metric attributes that can help you define routing conditions in your contact flows based on real-time metrics about the queues and agents in your contact center. When you include a Get queue metrics block in your contact flow, metrics are retrieved for the current working queue, or other queue that you specify, and returned as attributes that you can reference in blocks that occur after that block in the flow.

You can reference the metric attributes returned to determine the optimal route for a contact. Check the current queue metrics, such as the number of contacts or available agents in a queue, and how long the oldest contact has been in a queue. You could even get metrics for multiple queues and use a Set contact attributes block to store the metric attributes for each queue. You could then compare queue metric attributes using a Check contact attributes block, and route the contact to the queue with the fewest calls in it, or to a callback if all queues are busy. To learn more about the metric attributes available, see System Metrics Attributes (p. 99).

To use system metrics attributes in a contact flow
1. In Amazon Connect, choose Routing, Contact flows.
2. Select an existing contact flow, or create a new one.
3. Add a Get queue metrics block to the contact flow.
4. Optionally, to specify a queue select the Set queue check box and do one of the following:
   • Select the queue to retrieve metrics for from the drop-down list.
   • Select Use attribute, then select the attribute to use.
   If you do not select a queue, metrics are retrieved for the current working queue.
5. Add a Check contact attributes block and connect the Success branch of the Get queue metrics block to it.
6. Choose the title of the Check contact attributes block to display the properties for the block.
7. Under Attribute to check, in the Type drop-down menu, choose Queue metrics. In the Attribute drop-down menu, select the attribute to check.
8. To create a branching condition based on the value of the metric attribute, choose Add another condition.
9. For the Conditions to check, choose the conditions to compare the attribute value to, and then enter a value in the Value field.
10. Add additional blocks to the contact flow, connecting the branch of the Check contact attributes block to route the contact to the next block in the flow.
11. Save and publish the contact flow to make it available in your contact center.

System Attributes for Contact Flows

When creating a contact flow, 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.
• **Dialed number**—The number that the customer dialed to reach your contact center. This attribute is included in the CTRs and Lambda input under SystemEndpoint.

• **Customer callback number**—The number that the system uses to call the customer back, either for the Transfer to callback queue functionality, or for an agent dialing from the CCP. The default value is the number 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, either VOICE or CHAT.

• **Instance ARN**—The ARN for your Amazon Connect instance.

• **Initiation method**—Indicates how the contact was initiated. Valid values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, API, and QUEUE_TRANSFER.

**How to Use the Channel Contact Attribute**

You can personalize the customer's experience based on the channel they use to contact you. Here's what you do:

1. Add a Check contact attributes block to the beginning of your contact flow.

2. Configure the block as shown in the following image:
3. If the customer is contacting you through chat, specify what should happen next.

4. If the customer is contacting you through a call (No Match), specify the next step in the flow.

How to Use the Same Bot for Voice and Chat

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

1. In the Get customer input block, click the Amazon Lex tab.
2. Under Session attributes, choose Use attribute. Enter phoneNumber, and set to System, Customer Number, as shown in the following image.
3. Choose **Add another attribute**.

4. Select **Use attribute**. Enter **callType, System, Channel**, as shown in the following image.

5. Choose **Save**.

6. In your Lambda function you can access this value in the SessionAttributes field in the incoming event.
Contact Attributes Available in Amazon Connect

The following sections describe the contact attributes available in Amazon Connect.

**Contact Flow System Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer number</td>
<td>The customer's phone number.</td>
<td>System</td>
<td>$.CustomerEndpoint.Address</td>
</tr>
<tr>
<td>Dialed number</td>
<td>The number the customer dialed to call your contact center.</td>
<td>System</td>
<td>$.SystemEndpoint.Address</td>
</tr>
<tr>
<td>Customer callback number</td>
<td>The number to dial to call back the customer.</td>
<td>System</td>
<td>not applicable</td>
</tr>
<tr>
<td>Stored customer input</td>
<td>An attribute created from the most recent invocation of a <strong>Store customer input</strong> 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, either VOICE or CHAT.</td>
<td>System</td>
<td>$.Channel</td>
</tr>
<tr>
<td>Instance ARN</td>
<td>The ARN for your Amazon Connect instance.</td>
<td>System</td>
<td>$.InstanceARN</td>
</tr>
<tr>
<td>Initiation method</td>
<td>How the contact was initiated. Valid</td>
<td>System</td>
<td>$.InitiationMethod</td>
</tr>
</tbody>
</table>
Contact Attributes Available in Amazon Connect

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Endpoint Type</td>
<td>The type of the system endpoint. Valid value is TELEPHONE_NUMBER.</td>
<td>System</td>
<td>$.SystemEndpoint.Type</td>
</tr>
<tr>
<td>Customer Endpoint type</td>
<td>The type of the customer endpoint. Valid value is TELEPHONE_NUMBER.</td>
<td>System</td>
<td>$.CustomerEndpoint.Type</td>
</tr>
<tr>
<td>Queue Outbound Caller ID number</td>
<td>The outbound caller ID number defined for the queue. This can be useful for reverting the caller ID after setting a custom caller ID.</td>
<td>System</td>
<td>$.Queue.OutboundCallerId.Address</td>
</tr>
<tr>
<td>Queue Outbound Caller ID number type</td>
<td>The type of the outbound caller ID number. Valid value is TELEPHONE_NUMBER.</td>
<td>System</td>
<td>$.Queue.OutboundCallerId.Type</td>
</tr>
</tbody>
</table>

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.
### Contact Attributes Available in Amazon Connect

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialog state</td>
<td>The last dialog state returned from an Amazon Lex bot. The value is 'Fulfilled' if an intent was returned to the contact flow.</td>
<td>External</td>
<td>$.Lex.dialogState</td>
</tr>
<tr>
<td>Intent name</td>
<td>The user intent returned by Amazon Lex.</td>
<td>External</td>
<td>$.Lex.IntentName</td>
</tr>
<tr>
<td>Slots</td>
<td>Map of intent slots (key/value pairs) Amazon Lex detected from the user input during the interaction.</td>
<td>External</td>
<td>$.Lex.Slots.slotName</td>
</tr>
<tr>
<td>Session attributes</td>
<td>Map of key-value pairs representing the session-specific context information.</td>
<td>External</td>
<td>$.Lex.SessionAttributes.attributeKey</td>
</tr>
</tbody>
</table>

**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>$.Metrics.Queue.Size</td>
</tr>
<tr>
<td>Oldest contact in queue</td>
<td>For the contact that has been in the queue the longest, the length of</td>
<td>System</td>
<td>$.Metrics.Queue.OldestContactAge</td>
</tr>
</tbody>
</table>
### Contact Attributes Available in Amazon Connect

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>time that the contact has been in the queue, in seconds.</td>
<td>Agents online</td>
<td>The number of agents currently online, which means logged in and in any state other than offline.</td>
<td>System</td>
</tr>
<tr>
<td>The number of agents currently staffed, which is agents logged in and in Available, ACW, or Busy states.</td>
<td>Agents staffed</td>
<td>System</td>
<td>$.Metrics.Agents.Staffed.Count</td>
</tr>
<tr>
<td>The number of agents currently in the ACW state.</td>
<td>Agents in After contact work</td>
<td>System</td>
<td>$.Metrics.Agents.AfterContactWork.Count</td>
</tr>
<tr>
<td>The number of agents currently active on a contact.</td>
<td>Agents busy</td>
<td>System</td>
<td>$.Metrics.Agents.Busy.Count</td>
</tr>
<tr>
<td>The number of agents in the Missed state, which is the state an agent enters after a missed contact.</td>
<td>Agents missed count</td>
<td>System</td>
<td>$.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>The ARN of the Kinesis Video stream used for Live media streaming that includes the customer data to reference.</td>
<td>Customer audio stream ARN</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StreamARN</td>
</tr>
</tbody>
</table>
### Contact Attributes Available in Amazon Connect

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Type</th>
<th>JSONPath Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>used for Live media streaming.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer audio stop timestamp</td>
<td>When the customer audio stream stopped the Kinesis video stream used for Live media streaming.</td>
<td>Media streams</td>
<td>$.MediaStreams.Customer.Audio.StopTimestamp</td>
</tr>
<tr>
<td>Customer audio start fragment number</td>
<td>The number that identifies the Kinesis Video Streams fragment, in the stream used for Live media streaming, in which the customer audio stream started.</td>
<td>Media streams</td>
<td>$.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.
Set Up Your Network

Traditional VoIP solutions require you to allow both inbound and outbound for specific UDP port ranges and IPs, such as 80 and 443. These solutions also apply to TCP. In comparison, the network requirements for using the Contact Control Panel (CCP) with a softphone are less intrusive. You can establish persistent outbound send/receive connections through your web browser. As a result, you don’t need to open a client-side port to listen for inbound traffic.

The following diagram shows you what each port is used for.

The following sections describe the two primary connectivity options for using the CCP.

Option 1: Allow IP Address Ranges

The first option relies on using an allow list, also known as whitelisting, the IP addresses used by Amazon Connect. You create this allow list using the IP addresses in the AWS ip-ranges.json file. For more information about this file and IP address ranges in AWS, see AWS IP Address Ranges.

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available ip-ranges.json file. They are kept for a minimum of 30 days before they are used by the service.
After 30 days, softphone traffic through the new IP address ranges increases over the subsequent two weeks. After two weeks, traffic is routed through the new ranges equivalent to all available ranges.

<table>
<thead>
<tr>
<th>IP-Ranges entry</th>
<th>AWS Region</th>
<th>Ports/Protocols</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON_CONNECT</td>
<td>Region where your Amazon Connect instance is located</td>
<td>3478 (UDP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>EC2</td>
<td>Region where your Amazon Connect instance is located</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>CLOUDFRONT</td>
<td>Global*</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

*CloudFront serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range allow lists for CloudFront are global and require all IP ranges associated with "service": "CLOUDFRONT" in the ip-ranges.json file.

**Option 2: Replace Amazon EC2 and CloudFront IP Range Requirements with a Domain Allow List**

This second option lets you significantly reduce your blast radius.

We recommend trying Option 2 and testing it with more than 200 calls. Test for softphone errors, dropped calls, and conference/transfer functionality. If your error rate is greater than 2 percent, there might be an issue with proxy resolution. If that is the case, consider using Option 1.

<table>
<thead>
<tr>
<th>IP-Ranges entry</th>
<th>AWS Region</th>
<th>Ports/Protocols</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON_CONNECT</td>
<td>Region where the Amazon Connect instance is located</td>
<td>3478 (UDP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>

To allow traffic for Amazon EC2 endpoints, allow access for the URL and port, as shown in the first row of the following table. Do this instead of allowing all of the IP address ranges listed in the ip-ranges.json file. You get the same benefit using a domain for CloudFront, as shown in the second row of the following table.

<table>
<thead>
<tr>
<th>Domain/URL allow list</th>
<th>AWS Region</th>
<th>Ports</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtc.connect-telecom.{region}.amazonaws.com</td>
<td>Replace (region) with the Region where your Amazon Connect instance is located</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
<tr>
<td>{myInstanceName}.awsapps.com</td>
<td>Replace (myInstanceName) with the alias</td>
<td>443 (TCP)</td>
<td>OUTBOUND</td>
<td>SEND/RECEIVE</td>
</tr>
</tbody>
</table>
Domain/URL allow list | AWS Region | Ports | Direction | Traffic |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>of your Amazon Connect instance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tip**
When using `rtc.connect-telecom.{region}.amazonaws.com` and `https://myInstanceName.awsapps.com`, in certain proxy applications, web socket handling may impact functionality. Be sure to test and validate before deploying to a production environment.

**Stateless Firewalls**

If you’re using a stateless firewall for both options, use the requirements described in the previous sections. Then you must add to your allow list the ephemeral port range used by your browser, as shown in the following table.

<table>
<thead>
<tr>
<th>IP-Range entry</th>
<th>Port</th>
<th>Direction</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMAZON_CONNECT</td>
<td>49152-65535 (UDP)</td>
<td>INBOUND</td>
<td>SEND/REceive</td>
</tr>
</tbody>
</table>

**Port and Protocol Considerations**

Consider the following when implementing your network configuration changes for Amazon Connect:

- You need to allow traffic for all addresses and ranges for the Region in which you created your Amazon Connect instance.
- If you are using a proxy or firewall between the CCP and Amazon Connect, increase the SSL certificate cache timeout to cover the duration of an entire shift for your agents. Do this to avoid connectivity issues with certificate renewals during their scheduled working time. For example, if your agents are scheduled to work 8 hour shifts that include breaks, increase the interval to 8 hours plus time for breaks and lunch.
- When opening ports, Amazon EC2 and Amazon Connect require only the ports for endpoints in the same Region as your instance. CloudFront, however, serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range allow lists for CloudFront are global and require all IP ranges associated with "service": "CLOUDFRONT" in ip-ranges.json.
- Once ip-ranges.json is updated, the associated AWS service will begin using the updated IP ranges after 30 days. To avoid intermittent connectivity issues when the service begins routing traffic to the new IP ranges, be sure to add the new IP ranges to your allow list, within 30 days from the time they were added to ip-ranges.json.
- If you are using a custom CCP with the Amazon Connect Streams API, you can create a media-less CCP that does not require opening ports for communication with Amazon Connect, but still requires ports opened for communication with Amazon EC2 and CloudFront.

**Region Selection Considerations**

Amazon Connect Region selection is contingent upon data governance requirements, use case, services available in each Region, and latency in relation to your agents, contacts, and external transfer endpoint geography.
• **Agent location/network**—CCP connectivity traverses the public WAN, so it is important that the workstation has the lowest latency and fewest hops possible, specifically to the AWS Region where your resources and Amazon Connect instance are hosted. For example, hub and spoke networks that need to make several hops to reach an edge router can add latency and reduce the quality of experience.

When you set up your instance and agents, make sure to create your instance in the Region that is geographically closest to the Region where you create your instance. If you need to set up an instance in a specific Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your agent computers and your Amazon Connect instance.

• **Location of your callers**—Because calls are anchored to your Amazon Connect Region endpoint, they are subject to PSTN latency. Ideally your callers and transfer endpoints are geographically located as closely as possible to the AWS Region where your Amazon Connect instance is hosted for lowest latency.

For optimal performance, and to limit the latency for your customers when they call in to your contact center, create your Amazon Connect instance in the Region that is geographically closest to where your customers call from. You might consider creating multiple Amazon Connect instances, and providing contact information to customers for the number that is closest to where they call from.

• **External transfers**—from Amazon Connect remain anchored to your Amazon Connect Region endpoint for the duration of the call. Per-minute usage continues to accrue until the call is disconnected by the recipient of the transferred call. The call is not recorded after the agent drops or the transfer completes. The CTR data and associated call recording of a transferred call are generated after the call is terminated. Whenever possible, don't transfer calls that could be transferred back into Amazon Connect, known as circular transfers, to avoid compounding PSTN latency.

### Agents Using Amazon Connect Remotely

Remote agents, those that use Amazon Connect from a location other than those connected to your organization's main network, may experience issues relating to their local network if they have an unstable connection, packet loss, or high latency. This is compounded if a VPN is required to access resources. Ideally, the agents are located close to the AWS Region where your AWS resources and Amazon Connect instance are hosted, and have a stable connection to the public WAN.

### Rerouting Audio

When rerouting audio to an existing device, consider the location of the device in relation to your Amazon Connect Region. This is so you can account for potential additional latency. If you reroute your audio, whenever there is a call intended for the agent, an outbound call is placed to the configured device. When the agent answers the device, that agent is connected with the caller. If the agent does not answer their device, they are moved into a missed contact state until they or a supervisor changes their state back to available.

### Using AWS Direct Connect

Contact Control Panel (CCP) network connectivity issues are most often rooted in your route to AWS via private WAN/LAN, ISP, or both. While AWS Direct Connect does not solve issues specific to private LAN/WAN traversal to your edge router, it can help solve for latency and connectivity issues between your edge router and AWS resources. AWS Direct Connect provides a durable, consistent connection rather
than relying on your ISP to dynamically route requests to AWS resources. It also allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN.

Using Amazon Connect in a VDI Environment

Virtual Desktop Infrastructure (VDI) environments add another layer of complexity to your solution that warrants separate POC efforts and performance testing to optimize. The Amazon Connect Contact Control Panel (CCP) can operate in thick, thin, and zero client VDI environments as any other WebRTC based browser application does, and the configuration/support/optimization is best handled by your VDI support team. That being said, the following is a collection of considerations and best practices that have been helpful for our VDI-based customers.

- Location of your agents—Ideally, there are as few hops as possible with the lowest round trip time between the location from which your agents use the CCP and the VDI host location.
- Host location of your VDI solution—Ideally, your VDI host location is on the same network segment as your agents, with as few hops as possible from both internal resources as well as an edge router. You also want the lowest round-trip time possible to both WebRTC and Amazon EC2 range endpoints.
- Network—Each hop that traffic goes through between endpoints increases the possibility of failure and adds opportunity to introduce latency. VDI environments are particularly susceptible to call quality issues if the underlying route is not optimized or the pipe isn't either fast or wide enough. While AWS Direct Connect can improve call quality from the edge router to AWS, it will not address internal routing issues. You may need to upgrade or optimize your private LAN/WAN, or redirect to an external device to circumvent call audio issues. In most scenarios, if this is required, the CCP is not the only application that is having issues.
- Dedicated resources—at the Network and desktop level are recommended to prevent an impact to available agent resources from activities, such as backups and large file transfers. One way to prevent resource contention is by restricting the desktop access to Amazon Connect users who will be using their environment similarly, instead of sharing resources with other business units who may use those resources differently.
- Using a soft phone with remote connections—in VDI environments can cause impact to audio quality. If your agents connect to a remote endpoint and operates in that environment, we recommend either rerouting audio to an external E.164 endpoint or connecting the media through the local device and then signaling through the remote connection. You can build a custom CCP with the Amazon Connect Streams API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. For more information about the streams API, see the GitHub repository at https://github.com/aws/amazon-connect-streams.

CCP Connectivity

When an agent logs in, the CCP attempts to connect to the Amazon EC2 signaling endpoints listed in the AWS ipranges.json file. Amazon Connect for media, and CloudFront for web artifacts such as images. When the agent logs out or the browser is closed, endpoints are reselected when the agent next logs in. If a connection to Amazon EC2 or Amazon Connect fails, errors display on the CCP. If a connection to CloudFront fails, web elements such as buttons and icons, or even the page itself fails to load correctly.

Outbound calls

- When an outbound call is placed, the event signal is sent to the Amazon EC2 endpoint, which then communicates with Amazon Connect to place the call. Upon a successful dial attempt, the agent is bridged in, which anchors the call to the agent's Amazon Connect endpoint. Any external transfers or conferences also uses the anchor until the call is disconnected. Anchoring can help reduce PSTN latency.
Inbound calls

- When an inbound call is received, the call is anchored to an Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- When an agent is available, the call is pushed through via a new Amazon EC2 connection to their browser and offered to the agent.
- When the agent accepts the call and either the external device has been answered or the CCP determines it can receive a call, a connection to Amazon Connect is established for call media to the agent.

Transferred calls

- When a call is transferred, the transfer event that signals to place an outbound call to the specified transfer destination is sent to Amazon EC2, which then communicates with Amazon Connect to place the call.
- When the call is connected, the agent is bridged in, anchoring the call to the agent's existing Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- If the agent hangs up after the call is bridged, the agent's connection to the call is terminated, but Amazon Connect hangs on to the call at the Amazon Connect anchor point until there is a far side disconnect. When the call is disconnected, CTRs and associated recordings are generated and made available for the call.

Missed calls

- If the call is waiting on an agent, customer queue flow logic is used until an agent is available and the call has been successfully routed to that agent.
- If the agent does not accept the call, the agent moves into a Missed Call state and is unable to take calls until the agent, or a call center manager, changes their status to Available again. The caller does not hear ringing while the call is waiting for the agent, and continues to hold until connected with an agent as defined in the customer queue flow logic.

Panic logout

- If the browser window where the CCP is running is closed, the call remains connected, but opening the browser and logging back in will not allow you to re-establish the media connection. You are still able to transfer or end the call, but no audio path is established between the agent and caller.

Use an Allow List for Integrated Applications

All domains that embed the CCP for a particular instance must be explicitly allowed for cross-domain access to the instance. For example, to integrate with Salesforce, you must place your Salesforce Visualforce domain in an allow list.

To allow a domain URL

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from Instance Alias.
3. In the navigation pane, choose Application integration.
4. Choose Add origin.
5. Type the URL and choose Add.

107
Add an Amazon Lex Bot

In this article we guide you through the steps to add a Amazon Lex bot to Amazon Connect.

With Amazon Lex, you can build conversational interactions (bots) that feel natural to your customers. Amazon Connect with Amazon Lex bots can also capture customer input as digits that customers enter on their numeric keypad when used in an Amazon Connect contact flow. This way customers can choose how they want to enter sensitive information such as account numbers.

To follow along with this walkthrough, you need the following:

- An active AWS account.
- An Amazon Connect instance created in the US East (N. Virginia) Region. After you create your instance, claim a phone number for it.

Create an Amazon Lex Bot

In this step you’ll create a custom bot to demonstrate the Press or Say integration with Amazon Connect. The bot prompts callers to press or say a number that matches the menu option for the task to complete. In this case, the input is checking their account balance.

1. Open the Amazon Lex console.
2. If you are creating your first bot, choose Get Started. Otherwise, choose Bots, Create.
3. On the Create your Lex bot page, choose Custom bot and provide the following information:
   - Bot name – For this walkthrough, name the bot AccountBalance.
   - Output voice– Select the voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joana.
   - Session timeout- Choose how long the bot should wait to get input from a caller before ending the session.
   - COPPA– Choose whether the bot is subject to the Child Online Privacy Protection Act.
4. Choose Create.

Configure the Amazon Lex Bot

In this step you’ll determine how the bot responds to customers by providing intents, sample utterances, slots for input, and error handling.

Create Intents

For this example, you'll configure the bot with two intents: one to look up account information, and another to speak with an agent.

1. In the Amazon Lex console choose the + icon next to Intents, and choose Create new intent.
2. Name the intent AccountLookup.
3. Create another intent, and name it SpeakToAgent.

Add Sample Utterances

After defining the intents, add some sample utterances.
1. Select the **AccountLookup** intent.
2. Add a sample utterance, such as *Check my account balance*, and choose the + icon.
3. Add a second utterance, such as *One* and choose the + icon. This assigns the utterance of “one” or key press of “1” to the **AccountLookup** intent.

   **Tip**
   You must add an utterance of "one" in the bot, and not the number "1". This is because Amazon Lex doesn't support numeric input directly. To get around this, later in this walkthrough you'll use numeric input to interact with a Lex bot invoked from a contact flow.

4. Select **SpeakToAgent**.
5. Add a sample utterance, such as *Speak to an agent*, and choose +.
6. Add a second utterance, such as *Two*, and choose +.

### Add Slots

Before the bot can respond with the caller’s account balance, it needs the account number.

1. Choose the **AccountLookup** intent.
2. Under **Slots**, add a slot named **AccountNumber**.

3. For **Slot type**, use the drop-down to choose **AMAZON.NUMBER**.
4. For **Prompt**, add the text to be spoken when the call is answered. For example, ask callers to enter their account number using their keypad: *Using your touch-tone keypad, please enter your account number.*
5. Choose the + icon.
6. Make sure that the **Required** check box is selected.
Add Responses

Now that you have intents, utterances, and a slot, add the responses that the bot provides to callers. Because you are creating a simple bot for this example, you are not hooking up the bot to look up real customer data. The example bot responds with text strings that you add, regardless of the account number that a caller provides.

1. Select the AccountLookup intent.
2. In the Response section, add a message for the bot to say to customers. For example, “The balance for your account is $2,586.34.”
3. Choose Save Intent.
4. For the SpeakToAgent intent, add a message that lets callers know that their call is being connected to an agent. For example, “Okay, an agent will be with you shortly.”
5. Choose Save Intent.

Build and Test the Amazon Lex Bot

After you create your bot, make sure it works as intended before you publish it.

1. Choose Build. It may take a minute or two.
2. When it's finished building, choose Test Chatbot.
3. Let's test the AccountLookup intent: In the Test Chatbot pane, in the Chat with your bot box, type 1. Then type a fictitious account number.
Publish the Amazon Lex Bot and Create an Alias

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

1. Choose **Publish**.
2. Provide an alias for your bot. Use the alias to specify this version of the bot in the contact flow, for example, Test.
3. Choose **Publish**.

Add the Amazon Lex Bot to an Amazon Connect Instance

Before you can use a bot in your contact flow you need to add it to your Amazon Connect instance. You can only add bots created under the same AWS account.

If you add Amazon Lex bots created in a different Region from your instance, performance may be affected.

1. Open the Amazon Connect console.
2. Select the **Instance Alias** of the instance to which to add the bot.
3. Choose **Contact flows**.
4. Under **Amazon Lex**, use the drop-down to choose a name for your bot and then choose **+ Add Lex Bot**.

5. Select the **AccountBalance** bot and choose **Save Lex Bots**. If the name of your bot doesn't appear in the list, reload the page to get it to show up.

---

### Create a Contact Flow and Add Your Amazon Lex Bot

Next, create a new contact flow that uses your Amazon Lex bot. When you create the contact flow, you configure the message played to callers.

1. Log in to your Amazon Connect instance with an account that has permissions for contact flows and Amazon Lex bots.
2. Choose **Routing, Contact flows, Create contact flow**, and type a name for the flow.
3. Under **Interact**, drag a **Get customer input** block onto the designer, and connect it to the **Entry point block**.
4. Click the **Get customer input** block to open it. Choose **Text to speech (Ad hoc), Enter text**.
5. Type a message that provides callers with information about what they can do. For example, use a message that matches the intents used in the bot, such as "To check your account balance, press or say 1. To speak to an agent, press or say 2."
Add the Amazon Lex Bot to Your Contact Flow

In this step you'll specify the bot as the method of getting customer input.

1. In the Get customer input block select Amazon Lex.
2. For Name, use AccountBalance. For Alias, use Test.
3. Under **Intents**, choose **Add an intent**.
4. Type **AccountLookup** and choose **Add another intent**.

5. Type **SpeakToAgent** and choose **Save**.

### Finish the Contact Flow

After the caller interacts with the bot, finish the contact flow to complete the call for the customer.

1. If the caller presses 1 to get their account balance, use a **Prompt** block to play a message and disconnect the call.
2. If the caller presses 2 to speak to an agent, use a **Set queue** block to set the queue and transfer the caller to the queue, which ends the contact flow.

To complete the **AccountLookup** intent:

1. Under **Interact**, drag a **Play prompt block** to the designer, and connect the **AccountLookup** node of the **Get customer input** block to it. After the customer gets their account balance from the Amazon Lex bot, the message in the **Play prompt** block plays.
2. Under Terminate/Transfer, drag a Disconnect/hang up block to the designer, and connect the Play prompt block to it. After the prompt message plays, the call is disconnected.

To complete the SpeakToAgent intent:

1. Add a Set customer queue block and connect it to the SpeakToAgent node of the Get customer input block.
2. Add a Transfer to queue block.
3. Connect the Success node of the Set customer queue block to the Transfer queue.
4. Choose Save, then Publish.

Your finished contact flow will look something like the following one:

---

### Assign the Contact Flow to a Phone Number

When callers call in to your contact center, the contact flow to which they are sent is the one assigned to the telephone number that they dialed. To make the new contact flow active, assign it to a phone number for your instance.

1. Open the Amazon Connect Dashboard.
2. Choose View phone numbers.
3. Select the phone number to which to assign the contact flow.
4. Add a description.
5. In the Contact flow/IVR menu, choose the contact flow that you just created.
6. Choose Save.
Try It!

To try the bot and contact flow, call the number you assigned to the contact flow. Follow the prompts.
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. 117). 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-XXXXXXXXXXX",
      "CustomerEndpoint": {
         "Address": "+1234567890",
         "Type": "TELEPHONE_NUMBER"
      },
      "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
      "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
      "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/c8c0e68d-2200-4265-82c0-XXXXXXXXXXX",
      "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
      "queue": "QueueName",
      "SystemEndpoint": {
         "Address": "+1234567890",
         "Type": "TELEPHONE_NUMBER"
      }
   },
   "Parameters": {
      "sentAttributeKey": "sentAttributeValue"
   }
},
"Name": "ContactFlowEvent"
}
```

The request is divided into three parts:

- **Contact data**—This is always passed by Amazon Connect for every contact. Some parameters are optional.
- **User attributes**—These are attributes that have been previously associated with a contact, such as when using a **Set contact attributes** block in a contact flow. This map may be empty if there aren't any saved attributes.
- **Parameters**—These are parameters specific to this call that were defined when you created the Lambda function.
Invocation retry policy

If your Lambda invocation in a contact flow gets throttled, the request will be retried. It will also be retried if a general service failure (500 error) happens.

When a synchronous invocation returns an error, Amazon Connect retries up to 3 times, for a maximum of 8 seconds. At that point, the flow will progress down the Error branch.

To learn more about how Lambda retries, see Error Handling and Automatic Retries in AWS Lambda.

Invoke Multiple Lambda Functions

Amazon Connect limits the duration of a sequence of Lambda functions to 20 seconds. It will error out when the total execution time exceeds this threshold. Since customers hear silence while a Lambda function executes, we recommend adding a Play prompt block between functions to keep them engaged and aware of the long interaction.

By breaking up a chain of Lambda functions with the Play prompt block, you will be able to invoke multiple functions that last longer than the 20 second threshold.

Configure Your Lambda Function to Parse the Event

To successfully pass attributes between your Lambda function and Amazon Connect, configure your function to correctly parse the JSON request sent from the Invoke AWS Lambda function block, and define any business logic that should be applied. How the JSON is parsed depends on the runtime you use for your function. For example, the following example shows how to access sentAttributeKey using Node.JS:

```javascript
var receivedAttribute = event['Details']['Parameters']['sentAttributeKey'];
```

Verify the Function Response

The Lambda function response should be a simple string map. This map can be up to 32k. If you fail to reach Lambda, the function throws an exception, the response is not understood, or the Lambda function takes more time than the limit, the contact flow jumps to the Error label.

Test the output returned from your Lambda function to confirm that it will be correctly consumed when returned to Amazon Connect. The following example shows a sample response in Node.JS:

```javascript
exports.handler = function(event, context, callback) {
    var resultMap = {
        Name:'CustomerName',
        Address:'1234 Main Road',
        CallerType:'Patient'
    }
    callback(null, resultMap);
}
```

This example shows an example response using Python:
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 from the most recently invoked function. To use the response from a function before a subsequent function is invoked, the response must be saved as a contact attribute, or passed as a parameter to the next function.

**Access Variables Directly**

If you access the variables directly, you can use them in contact flow blocks, but they are not included in contact trace records (CTR). To access these variables directly in a contact flow block, add the block after the Invoke AWS Lambda function block, and then reference the attributes as shown in the following example:

```
Name - $.External.Name
Address - $.External.Address
CallerType - $.External.CallerType
```

Make sure that the name specified for the source attribute matches the key name returned from Lambda.

**Store Variables as Contact Attributes**

If you store the variables as contact attributes, you can use them throughout your contact flow, and they are included in CTRs.

To store the values returned as contact attributes and then reference them, use a Set contact attributes block in your contact flow after the Invoke AWS Lambda function block. Choose External for the Type. Following the example we're using, set Destination key to returnedContactName, and set the Source attribute to Name.

Add Address as a Source attribute and use returnedContactAddress as the Destination key. Then add callerType as a Source attribute and use returnedContactType for the Destination key.

Make sure that the name specified for the source attribute matches the key name returned from Lambda.
Encrypt Customer Input

You can encrypt sensitive data that is collected by contact flows. To do this, you need to use public-key cryptography. Here's how this works:

In a contact flow that collects data, you provide an X.509 certificate to encrypt data that's captured using the Stored customer input system attribute. You must upload a signing key in .pem format 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.

To decrypt the data in the Stored customer input attribute, use the AWS Encryption SDK. For more information, see the AWS Encryption SDK Developer Guide.

For a detailed walkthrough, see Creating a secure IVR solution with Amazon Connect. It shows how to:

- Configure Amazon Connect to collect a credit card number.
- Encrypt the credit card digits.
- Send it to our backend AWS Lambda for decryption, using the customer supplied decryption key.
Capture Customer Audio: Live Media Streaming

In Amazon Connect, you can capture customer audio during an interaction with your contact center by sending the audio to a Kinesis video stream. Depending on your settings, audio can be captured for the entire interaction—until the interaction with the agent is complete—or only one direction:

- What the customer hears, including what the agent says and system prompts.
- What the customer says, including when they are on hold.

The customer audio streams also include interactions with an Amazon Lex bot, if you're using one in your contact flow.

You can perform analysis on the audio streams to determine customer sentiment, use the audio for training purposes, or to later review the audio to identify and flag abusive callers.

Contents

- Plan for Live Media Streaming (p. 122)
- Enable Live Media Streaming in Your Instance (p. 123)
- How to Access Kinesis Video Streams Data (p. 123)
- Example Contact Flow for Testing Live Media Streaming (p. 128)
- Contact Attributes for Live Media Streaming (p. 130)

Plan for Live Media Streaming

You can send all audio to and from the customer to Kinesis Video Streams. Media streaming leverages Kinesis Video Streams multi-track support so that what the customer says is on a separate track from what the customer hears.

Audio sent to Kinesis uses a sampling rate of 8 Khz.

Do You Need to Increase Your Service Limits?

When you enable media streaming in Amazon Connect, one Kinesis video stream is used per active call. By default we allocate 50 streams to your account. We automatically create additional streams as needed to keep pace with active calls, unless your account reaches the Kinesis Video Streams service limit.

Check out the default Kinesis service limit for number of streams per account for your region (see the limit for the CreateStream API).

To make sure that there are enough streams available for all calls in your contact center, the value of the CreateStream API needs to be greater than the number of the maximum concurrent active calls for your instance.

If you have more than one instance for your AWS account, your CreateStream limit should be a number greater than the concurrent active calls for all of your instances combined.

To request an increase to your service limit, in the AWS Support Center, choose Create Case and then choose Service Limit Increase.
Tip
We make sure that PutMedia requests always stay within the 5 TPS limit. You don’t need to request an increase.

How Long Do You Need to Store Audio?

Customer audio is stored in Kinesis for the time defined by your retention settings in an Amazon Connect instance. For instructions for setting this value, see Enable Live Media Streaming in Your Instance (p. 123).

Who Requires IAM Permissions to Retrieve Data?

If your business is using IAM policies and permissions, the IAM admin will need to grant permissions to people who are going to retrieve data from Kinesis Video Streams. They’ll need to grant them full access permissions for Kinesis Video Streams and AWS Key Management Service.

Enable Live Media Streaming in Your Instance

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

To enable live media streaming

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the instance alias for the instance from the Instance Alias column.
3. In the navigation pane, choose Data storage.
5. Enter a prefix for the Kinesis Video Streams created for your customer audio. This prefix makes it easier for you to identify the stream with the data.
6. Choose the KMS master key to use to encrypt the data sent to Kinesis.
7. Specify a number and unit for the Data retention period. If you select No data retention, data is not retained and can be used only for immediate consumption.
8. Choose Save under Live media streaming, and then choose Save at the bottom of the page.

After you enable live media streaming, add Start media streaming and Stop media streaming blocks to your contact flow. Configure those blocks to specify what audio you want to capture. For instructions and an example, see Example Contact Flow for Testing Live Media Streaming (p. 128).

How to Access Kinesis Video Streams Data

You must have developer skills to work with Kinesis Video Streams data. Use the steps and code samples in this section to interact with the customer audio data sent to Kinesis Video Streams.

Get Started with a Sample

There’s an example project on GitHub to help you to get started using Amazon Connect live audio streaming and real-time transcription using Amazon Transcribe. See Amazon Connect Real-time Transcription Lambda.
This project provides a code example and a fully functional Lambda function. They help you get started capturing and transcribing Amazon Connect phone calls using Kinesis Video Streams and Amazon Transcribe.

You can use the Lambda function in this project to create other solutions, such as:

- Capturing audio in the IVR.
- Providing real-time transcription to agents.
- Creating a voicemail solution for Amazon Connect.

## Build Your Own Implementation

You may want to implement a solution other than the one provided by the previously-described sample. If so, this section describes how to make the proper API calls against the Kinesis Video Streams so you can build your own solution from scratch.

1. Go to this GitHub page, and read about the Amazon Connect Real-time Transcription Lambda project.
2. Choose the deployment folder, and download the cloudformation.template.
3. Use the following example Java classes, which are built on top of the Kinesis video parser library using the AWS SDK for Java.
   - **LMSDemo** — is a class with a main method that invokes LMSExample.
   - **LMSExample** — is similar to the examples provided in the Kinesis Video Streams Parser library. It gets media from the specified Kinesis Video Streams with the specified fragment number. This code sample includes frame processing to separate the tracks.
   - **LMSFrameProcessor** — is invoked by LMSExample to save data from Kinesis Video Streams to the specified output stream. Use a file output stream to save the output to a file. This code sample also includes frame processing to separate the tracks.
4. Use Audacity, or other audio tool, to import the .raw audio file, which is in a 16-bit signed PCM Mono format.

### Code Samples to Access Kinesis Video Streams Data

#### LMSDemo.java

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

import com.amazonaws.auth.AWSSessionCredentials;
import com.amazonaws.auth.AWSSessionCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.kinesisvideo.parser.examples.LMSExample;
import com.amazonaws.regions.Regions;
import java.io.FileOutputstream;
import java.io.IOException;
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() {
    }
}

public class LMSExample extends KinesisVideoCommon {

    private final ExecutorService executorService;
    private GetMediaProcessingArguments getMediaProcessingArguments;

    public LMSExample() {
        executorService = Executors.newFixedThreadPool(5);
    }

    public void startProcessing() {
        executorService.submit(new LMSFrameProcessor(getMediaProcessingArguments, new FragmentMetadataVisitor(), new FrameVisitor(), new LMSFrameProcessor() {
            @Override
            public void processFrame(MkvDataElement dataElement) {
                // Process the frame
            }
        }, new MkvTypeInfos(), new MkvElementVisitor()));
    }

    public void stopProcessing() {
        executorService.shutdown();
    }

    public static void main(String[] args) throws IOException, InterruptedException, MkvElementVisitException, FileNotFoundException {
        LMSExample example = new LMSExample();
        example.startProcessing();
        example.stopProcessing();
    }

    // Other methods and classes
}

LMSExample.java
private final StreamOps streamOps;
private final OutputStream outputStreamFromCustomer;
private final OutputStream outputStreamToCustomer;
private final String fragmentNumber;

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

public void execute () throws InterruptedException, IOException {
        GetMediaProcessingArguments = GetMediaProcessingArguments.create(outputStreamFromCustomer, outputStreamToCustomer);
        try (GetMediaProcessingArguments getMediaProcessingArgumentsLocal = getMediaProcessingArguments) {
            //Start a GetMedia worker to read and process data from the Kinesis Video Stream.
            GetMediaWorker getMediaWorker = GetMediaWorker.create(getRegion(),
                    getCredentialsProvider(),
                    getStreamName(),
                    new StartSelector().withStartSelectorType(StartSelectorType.FRAGMENT_NUMBER).withAfterFragmentNumber(fragmentNumber),
                    streamOps.amazonKinesisVideo,
                    getMediaProcessingArgumentsLocal.getFrameVisitor());
            executorService.submit(getMediaWorker);
            //Wait for the workers to finish.
            executorService.awaitTermination(120, TimeUnit.SECONDS);
            if (!executorService.isTerminated()) {
                System.out.println("Shutting down executor service by force");
                executorService.shutdownNow();
            } else {
                System.out.println("Executor service is shutdown");
            }
        } finally {
            outputStream.close();
        }
    }

private static class LogVisitor extends MkvElementVisitor {
    private final FragmentMetadataVisitor fragmentMetadataVisitor;
    private LogVisitor(FragmentMetadataVisitor fragmentMetadataVisitor) {
        this.fragmentMetadataVisitor = fragmentMetadataVisitor;
    }
    public long getFragmentCount() {
        return fragmentCount;
    }
    private long fragmentCount = 0;
    @Override
    public void visit(MkvStartMasterElement startMasterElement) throws MkvElementVisitException {

if (MkvTypeInfos.EBML.equals(startMasterElement.getElementMetaData().getTypeInfo())) {
    fragmentCount++;
    System.out.println("Start of segment");
}

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

private static class GetMediaProcessingArguments implements Closeable {
    public FrameVisitor getFrameVisitor() {
        return frameVisitor;
    }

    private final FrameVisitor frameVisitor;

    public GetMediaProcessingArguments(FrameVisitor frameVisitor) {
        this.frameVisitor = frameVisitor;
    }

    public static GetMediaProcessingArguments create(OutputStream
      outputStreamFromCustomer, OutputStream outputStreamToCustomer) throws IOException {
        //Fragment metadata visitor to extract Kinesis Video fragment metadata from the
        GetMedia stream.
        FragmentMetadataVisitor fragmentMetadataVisitor = FragmentMetadataVisitor.create();

        //A visitor used to log as the GetMedia stream is processed.
        LogVisitor logVisitor = new LogVisitor(fragmentMetadataVisitor);

        //A composite visitor to encapsulate the three visitors.
        FrameVisitor frameVisitor = FrameVisitor.create(LMSFrameProcessor.create(outputStreamFromCustomer,
          outputStreamToCustomer, fragmentMetadataVisitor));

        return new GetMediaProcessingArguments(frameVisitor);
    }

    @Override
    public void close() throws IOException {
    }
}

LMSFrameProcessor.java

package com.amazonaws.kinesisvideo.parser.utilities;
Example Contact Flow for Testing Live Media Streaming

Here's how you can set up a contact flow to test live media streaming:

```java
import com.amazonaws.kinesisvideo.parser.mkv.Frame;
import com.amazonaws.kinesisvideo.parser.utilities.FragmentMetadataVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.MkvTrackMetadata;
import java.io.IOException;
import java.io.OutputStream;
import java.nio.ByteBuffer;

public class LMSFrameProcessor implements FrameVisitor.FrameProcessor {
    private OutputStream outputStreamFromCustomer;
    private OutputStream outputStreamToCustomer;
    private FragmentMetadataVisitor fragmentMetadataVisitor;

    protected LMSFrameProcessor(OutputStream outputStreamFromCustomer, OutputStream outputStreamToCustomer, FragmentMetadataVisitor fragmentMetadataVisitor) {
        this.outputStreamFromCustomer = outputStreamFromCustomer;
        this.outputStreamToCustomer = outputStreamToCustomer;
    }

    public static LMSFrameProcessor create(OutputStream outputStreamFromCustomer, OutputStream outputStreamToCustomer, FragmentMetadataVisitor fragmentMetadataVisitor) {
        return new LMSFrameProcessor(outputStreamFromCustomer, outputStreamToCustomer, fragmentMetadataVisitor);
    }

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

    private void saveToOutputStream(final Frame frame) {
        ByteBuffer frameBuffer = frame.getFrameData();
        long trackNumber = frame.getTrackNumber();
        MkvTrackMetadata metadata = fragmentMetadataVisitor.getMkvTrackMetadata(trackNumber);
        String trackName = metadata.getTrackName();
        try {
            byte[] frameBytes = new byte[frameBuffer.remaining()];
            frameBuffer.get(frameBytes);
            if (Strings.isNullOrEmpty(trackName) ||
                "AUDIO_FROM_CUSTOMER".equals(trackName)) {
                outputStreamFromCustomer.write(frameBytes);
            } else if ("AUDIO_FROM_CUSTOMER".equals(trackName)) {
                outputStreamToCustomer.write(frameBytes);
            } else {
                // Unknown track name. Not writing to output stream.
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```
1. Add a **Start media streaming** block at the point where you want to enable customer audio streaming.

2. Connect the **Success** branch to the rest of your flow.

3. Add a **Stop media streaming** block to where you want to stop streaming.

4. Configure both blocks to specify what you want to stream: **From the customer** and/or **To the customer**.

Customer audio is captured until a **Stop media streaming** block is invoked, even if the contact is passed to another contact flow.

Use the contact attributes for media streaming in your contact flow so that the CTR includes the attributes. You can then view the CTR to determine the media streaming data associated with a specific contact. You can also pass the attributes to an AWS Lambda function.

The following example contact flow shows how you might use media streaming with attributes for testing purposes.
After the audio is successfully streamed to Kinesis Video Streams, the contact attributes are populated from the **Invoke AWS Lambda function** block. You can use the attributes to identify the location in the stream where the customer audio starts. For instructions, see Contact Attributes for Live Media Streaming (p. 130).

**Contact Attributes for Live Media Streaming**

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.
**getJSONPath format:** $.MediaStreams.Customer.Audio.StreamARN
Customer audio start timestamp
The time at which the customer audio stream started.

**getJSONPath format:** $.MediaStreams.Customer.Audio.StartTimestamp
Customer audio stop timestamp
The time at which the customer audio stream stopped.

**getJSONPath 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.

**getJSONPath 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.

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

For more information about Amazon Kinesis Video Streams fragments, see Fragment in the Amazon Kinesis Video Streams Developer Guide.
Integrate With Your CRM

You can integrate Amazon Connect with 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 Streams. When completed, add the origin URLs to your instance settings. This enables communication between Amazon Connect and your CRM. For more information, see Use an Allow List for Integrated Applications (p. 107).

Contents
- Amazon Connect and Salesforce Integration (p. 132)
- Amazon Connect and Zendesk Integration (p. 134)

Amazon Connect and Salesforce Integration

The core functionality of the Amazon Connect CTI Adapter provides a WebRTC browser-based Contact Control Panel (CCP) within Salesforce. The Amazon Connect CTI integration consists of two components:

- A managed Salesforce package.
- An AWS Serverless application deployed to your AWS environment.

With those components, you 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.

Amazon Connect CTI Adapter v4 for Salesforce Installation Guide

For a detailed walk-through and setup of the full CTI Adapter capabilities, see the Amazon Connect CTI Adapter v4 for Salesforce installation guide. We also have a trailhead available at https://sfdc.co/Amazon-Connect.

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.

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/).
- 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. This means users are required to use the latest version of either Google Chrome or Mozilla Firefox.

Quick Setup for a Sandbox Environment

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).
   - 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. Put your Salesforce Visualforce domain URL on an allow list using the directions in Use an Allow List for Integrated Applications (p. 107). 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).

Known Issue

Upon the completion of a call, Amazon Connect puts the agent into the After Contact Work state. As part of the Adapter, a Call Wrap-Up page will be triggered in Salesforce. When you integrate Amazon Connect with Salesforce Classic, this page will not be triggered.

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.**

Amazon Connect and Zendesk Integration

To integrate Amazon Connect and Zendesk, you need:

- An Amazon Connect instance.
- A Zendesk Support account with a Zendesk Talk Partner Edition plan, or a Zendesk trial account.

Install and configure the Amazon Connect for Zendesk app in your Zendesk Support account, then integrate the app with Amazon Connect. After integration, you can create contact flows to use Amazon Connect with Zendesk ticketing.

For more information, see the Amazon Connect Zendesk Integration User Guide and How do I integrate Amazon Connect with Zendesk?
Manage Users in Amazon Connect

As the admin one of your key responsibilities will be to manager users: add users to Amazon Connect give them their credentials, and assign the appropriate permissions so they can access the features needed to do their job.

Contents
• Add Users (p. 135)
• Reset a User's Password (p. 135)
• Assign Permissions: Security Profiles (p. 136)
• Use Service-Linked Roles for Amazon Connect (p. 137)
• Controlling Access with AWS Identity and Access Management (p. 139)

Add 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 Assign Permissions: Security Profiles (p. 136). Contacts can be routed based on the skills required of the agents. For more information, see Create a Routing Profile (p. 42).

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 add several users from an Excel spreadsheet (.csv)
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 Upload my users from a template (csv) and then choose Next.
5. Choose Download template.
6. Add your users to the template and upload it to Amazon Connect.

Reset a User's Password

To reset a password for a user
1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Users, User management.
3. Select the user and choose Edit.
4. Choose **reset password**. Specify a new password and then choose **Submit**.

   Resetting the user's password will immediately log them out of the contact control panel.

5. Communicate the new password to the user.

### Assign Permissions: 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, manage conversations, recordings of conversations, 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 contacts, they will see an icon to download recordings.

  **Important**

  This setting isn't a security feature. Users who don't have this permission can still download recordings using other less-discoverable ways.

### 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).
2. Choose **Users, Security profiles**.
3. Choose **Add new security profile**.
4. Type a name and description for the security profile.
5. Choose the appropriate permissions for the security profile from each permission group. For each permission type, choose one or more actions. Selecting some actions results in other actions being selected. For example, selecting **Edit** also selects **View** for the resource and any dependent resources.
6. Choose **Save**.

### 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).
2. Choose **Users, Security profiles**.
3. Select the name of the profile.
4. Update the name, description, and permissions as needed.
5. Choose **Save**.

### 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**.

### Use Service-Linked Roles for Amazon Connect

Amazon Connect uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Connect. Service-linked roles are
predefined by Amazon Connect and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon Connect easier because you don't have to manually add the necessary permissions. Amazon Connect defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Connect can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-Linked Role Permissions for Amazon Connect

Amazon Connect uses the service-linked role named AWSServiceRoleForAmazonConnect_ – Grants Amazon Connect permission to access AWS resources on your behalf.

The AWSServiceRoleForAmazonConnect_ service-linked role trusts the following services to assume the role:

- connect.amazonaws.com

The role permissions policy allows Amazon Connect to complete the following actions on the specified resources. As you enable additional features in Amazon Connect, additional permissions are added for the service-link role to access the resources associated with those features:

- Action: all Amazon Connect actions, connect:* , on all Amazon Connect resources.
- Action: Amazon S3 s3:GetObject, s3:GetObjectAcl, s3:PutObject, s3:PutObjectAcl, s3:DeleteObject, s3:GetBucketLocation, and GetBucketAcl for the S3 bucket specified for recorded conversations.

  It also grants s3:PutObject, s3:PutObjectAcl, and s3:GetObjectAcl to the bucket specified for exported reports.
- Action: Amazon Kinesis Data Firehose firehose:DescribeDeliveryStream and firehose:PutRecord, and firehose:PutRecordBatch for the delivery stream defined for Agent event streams and CTRs.
- Action: Amazon Kinesis Data Streams kinesis:PutRecord, kinesis:PutRecords, and kinesis:DescribeStream for the stream specified for Agent event streams and CTRs.
- Action: Amazon Lex lex:PostContent for the bots added to your instance.
- Action: Amazon CloudWatch Logs logs:CreateLogStream, logs:DescribeLogStreams, and logs:PutLogEvents to the CloudWatch Logs group specified for contact flow logging.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a Service-Linked Role for Amazon Connect

You don't need to manually create a service-linked role. When you create a new instance in Amazon Connect in the AWS Management Console, Amazon Connect creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new instance in Amazon Connect, Amazon Connect creates the service-linked role for you again.
You can also use the IAM console to create a service-linked role with the Amazon Connect - Full access use case. In the IAM CLI or the IAM API, create a service-linked role with the connect.amazonaws.com service name. For more information, see Creating a Service-Linked Role in the IAM User Guide. If you delete this service-linked role, you can use this same process to create the role again.

Editing a Service-Linked Role for Amazon Connect

Amazon Connect does not allow you to edit the AWSServiceRoleForAmazonConnect_ service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

Checking a Service-Linked Role Has Permissions for Amazon Lex

1. In the navigation pane of the IAM console, choose Roles.
2. Choose the name of the role to modify.

Deleting a Service-Linked Role for Amazon Connect

You don't need to manually delete the AWSServiceRoleForAmazonConnect_ role. When you delete your Amazon Connect instance in the AWS Management Console, Amazon Connect cleans up the resources and deletes the service-linked role for you.

Supported Regions for Amazon Connect Service-Linked Roles

Amazon Connect supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.

Controlling Access with AWS Identity and Access Management

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. For people who access Amazon Connect APIs, you can create IAM users. This enables you to manage at a granular level what these users can do with Amazon Connect, such as whether they can create or delete an instance.

You can also manage what other AWS services and resources are available to each IAM user. For more information about all the services that you can control access to, see AWS Services that Support IAM in the IAM User Guide.

Amazon Connect Actions

When you create an IAM user or group in your AWS account, you can associate an IAM policy with that group or user, which specifies the permissions that you want to grant.
For example, imagine you have a group of entry-level developers. You can create an IAM group named `Junior application developers`, and include all entry-level developers. Then, associate a policy with that group that grants them permissions to view Amazon Connect users. In this scenario, you might have a policy such as the following sample.

**Sample policy that grants "view user" permissions to IAM users**

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "connect:DescribeUser",
            "connect:ListUsers"
         ],
         "Resource": "*"
      }
   ]
}
```

This sample policy grants permissions to API actions listed in the `Action` element.

**Note**

If you don't specify a user ARN or ID in your statement, you must also grant the permission to use all resources for the action using the * wildcard for the `Resource` element.

---

**Amazon Connect Resources**

Amazon Connect supports resource-level permissions for IAM users, so you can specify actions for them for an instance, as shown in the following policy.

**Sample policy that denies the "delete" and "update" actions for users in one instance**

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "connect:DeleteUser",
            "connect:UpdateUser*
         ],
         "Resource": "arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/agent/*"
      }
   ]
}
```

This sample policy uses a wild card at the end of the Amazon Connect user ARN so that "delete user" and "update user" are denied on the full user ARN (that is, all Amazon Connect users in the provided instance, such as `arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/agent/00dtcddd1-123e-111e-93e3-11111bfbfcc1`).
Sample policy that allows "create users" but denies if you're assigned to a specific security profile

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["connect:CreateUser"],
         "Resource": "*",
      },
      {
         "Effect": "Deny",
         "Action": ["connect:CreateUser"],
      }
   ]
}
```

This sample policy allows "create users" but explicitly denies using arn:aws:connect:us-west-2:123456789012:instance/00fbeee1-123e-111e-93e3-11111bffcc17/security-profile/11dtcgggl-123e-111e-93e3-11111bffcc17 as the parameter for security profile in CreateUser request.

Amazon Connect Conditions

In an IAM policy, you can optionally specify conditions that control when a policy is in effect. For example, you can define a policy that allows IAM users to update only an Amazon Connect user who is working in the test environment.

You can define some conditions that are specific to Amazon Connect, and define other conditions that apply to all of AWS. For more information and a list of AWS-wide conditions, see Condition in IAM JSON Policy Elements Reference in the IAM User Guide.

Sample policy that allows the "describe" and "update" actions for users with specific tags

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["connect:DescribeUser", "connect:UpdateUser*"],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:ResourceTag/Department": "Test"
            }
         }
      }
   ]
}
```
This policy allows "describe user" and "update user" but only for those Amazon Connect users tagged with tag "Department: Test" where "Department" is the tag key and "Test" is the tag value.

Sample policy that allows the create actions for users with specific request tags

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "connect:CreateUser",
        "connect:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Owner": "TeamA"
        }
      }
    }
  ]
}
```

This policy allows "create user" and "tag resource" but the tag "Owner: TeamA" must be present in the requests.
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. 146).

**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. 150).

**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. 163).

**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. 165).

Monitor Live Conversations

Managers can monitor live conversations between agents and customers, and review past conversations. To set this up, you need to add the Set recording behavior block to your contact flow, assign managers the appropriate permissions, and then show them how to monitor the conversations.

A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the IVR.

**Important**

For voice conversations, the monitor feature works only when recording is enabled on a contact flow. For instructions, see Set Up Recording Behavior (p. 69).

For chat conversations, you enable recording at the instance level. If there's an S3 bucket for storing chat transcripts, then all chats are recorded. If no bucket exists, then no chats are recorded.

Assign Permissions to Monitor Live Conversations

These permissions enable managers to monitor live conversations and access recordings of past conversations.

**To assign a manager permissions to monitor a live conversation**

1. Go to Users, User management, choose the manager, and then choose Edit.
2. In the Security Profiles box, assign the manager to the **CallCenterManager** security profile. This security profile also includes a setting that makes the icon to download recordings appear in the results of the Contact search page.
3. Assign the manager to the **Agent** security profile so they can access the contact control panel. This is so they can monitor the conversation through the contact control panel.
4. Choose Save.
Or, to create a new security profile specific for this purpose

1. Choose **Users**, **User management**, **Security profiles**.
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**.

Monitor Live Conversations with Contacts

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 contact control panel (CCP) by choosing the phone icon in the top-right corner of your screen. You’ll need the CCP open to connect to the conversation.
3. To choose the agent conversation you want to monitor, in Amazon Connect choose **Metrics and quality**, **Real-time metrics**, **Agents**.
4. To monitor voice conversations: Next to the names of agents in a live voice conversation, you’ll see a headset icon. Choose the icon to start monitoring the conversation. When you’re monitoring a conversation, the status in your CCP changes to **Monitoring**.
5. To monitor chat conversations: For each agent you’ll see the number of live chat conversations they’re in. Click on the number. Then choose the conversation you want to start monitoring. When you’re monitoring a conversation, the status in your CCP changes to **Monitoring**.
6. To stop monitoring the conversation, in the CCP choose **End call** or **End chat**. When the agent ends the conversation, monitoring stops automatically.

Review Recorded Conversations

Managers can review past conversations between agents and customers. To set this up, you need to set up recording behavior (p. 69), assign managers the appropriate permissions, and then show them how to access the recorded conversations.

A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the IVR.

**Important**
For voice conversations, the monitor feature works only when recording is enabled on a contact flow. For instructions, see Set Up Recording Behavior (p. 69).
For chat conversations, you enable recording at the instance level. If there’s an S3 bucket for storing chat transcripts, then all chats are recorded. If no bucket exists, then no chats are recorded.

Assign Permissions to Review Recordings of Past Conversations

These permissions enable managers to access recordings of past conversations.
To assign a manager permissions to review recordings of past conversations

1. Go to **Users, User management**, choose the manager, and then choose **Edit**.
2. In the Security Profiles box, assign the manager to the **CallCenterManager** security profile. This security profile also includes a setting that makes the icon to download recordings appear in the results of the Contact search page.
3. If you also want the manager to monitor live conversations, assign the manager to the **Agent** security profile so they can access the Contact Control Panel. This is so they can monitor the conversation through the Contact Control Panel.
4. Choose **Save**.

**Or, to create a new security profile specific for this purpose**

1. Choose **Users, User management, Security profiles**.
2. Choose **Add new security profile**.
3. Expand **Metrics and Quality**, then choose **Manager monitor and Recorded conversations** (choose both **Access** and **Enable download button**).
4. If you also want the manager to monitor live conversations, assign the manager to the **Agent** security profile so they can access the Contact Control Panel. This is so they can monitor the conversation through the Contact Control Panel.
5. Choose **Save**.

**Review or Download Recordings/Transcripts of Past Conversations**

These are the steps that a manager does to review or download past recordings/transcripts of conversations.

1. Log in to Amazon Connect 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. Conversations that were recorded will have icons in the Recording column. Click to review the recording, download, or delete it. If you choose to download the recording, it will be saved automatically to your Downloads folder.

Here's what a sample transcript looks like:
Search for Recordings by Contact ID

To find a recording of a specific contact, you only need the contact ID. You don’t need to know the date range, agent, or any other information about the contact.

1. Log in to Amazon Connect with a user account that is assigned the CallCenterManager security profile, or that is enabled for the Contact search and Manager monitor permissions.
2. In Amazon Connect choose Metrics and quality, Contact search.
3. In the Contact ID, enter the contact ID, and then choose Search.
4. Conversations that were recorded will have icons in the Recording column. If you don’t have Manager monitor permissions, you won’t see this icon (or be able to review the recordings).

To learn more about searching, see Contact Search (p. 199).

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. 147).

- 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. 147).

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 Login_Logout report.csv is downloaded to your computer.

Share a Login/Logout Report

To make the report available to other people in your organization, you can share a report. People can
access the report only if they have appropriate permissions in Amazon Connect.
To share a Login/Logout report

1. On the Login/Logout report page, at the top right corner, choose the Share report menu (arrow) next to Save.
2. Choose Share report.
3. To copy the URL to the report, choose Copy link address. You can send the URL to others in your organization by pasting the link into an email or other document.
4. To publish the report to your organization, for Publish report to organization, move the toggle to On.
5. Choose Save.

Schedule a Login/Logout Report

To generate a report with the same settings on a regular basis, you can schedule the report to run daily or on specific days of the week. When you schedule a report, it is automatically published to your organization. Anyone with appropriate permissions can view the report. Users with all permissions for Login/Logout reports can also edit, schedule, or delete the report.

When you schedule your report, keep in mind that the report always runs at 12AM on the day you select, in the time zone that you choose. If you select Wednesday, the report runs at midnight Wednesday and does not include any data for Wednesday. Scheduled reports are saved as CSV files in your Amazon S3 bucket. The default time zone is UTC. To have your report run at 12AM in your local time, choose your time zone instead.

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 these CCP events:

- Agent login
- Agent logout
- Agent connects with a contact
- Agent status change, such as to Available to handle contacts, or on Break or at Training.

You can use the agent event streams to create dashboards that display agent information and events, integrate streams into workforce management (WFM) solutions, and configure alerting tools to trigger custom notifications of specific agent activity. Agent event streams help you manage agent staffing and efficiency.

Contents

- Enable Agent Event Streams (p. 150)
- Sample Agent Event Stream (p. 151)
- Determine How Long an Agent Spends Doing ACW (p. 153)
- Agent Event Streams Data Model (p. 158)

Enable Agent Event Streams

Agent event streams are not enabled by default. Before you can enable agent event streams in Amazon Connect, create a data stream in Amazon Kinesis Data Streams. Then, choose the Kinesis stream as the stream to use for agent event streams. Though you can use the same stream for both agent event streams and contact trace records, managing and getting data from the stream is much easier when you use a separate stream for each. For more information, see the Amazon Kinesis Data Streams Developer Guide.

When data is sent to Kinesis, the partition key used is the agent ARN. All events for a single agent are sent to the same shard, and any resharding events in the stream are ignored.

Note

If you enable server-side encryption for the Kinesis stream you select for agent event streams, Amazon Connect cannot publish to the stream. This is because it does not have permission to Kinesis kms:GenerateDataKey. To work around this, first enable encryption for scheduled
reports or recordings of conversations. Next, create a customer master key (CMK) using KMS for encryption. Finally, choose the same CMK for your Kinesis data stream that you use for encryption of scheduled reports or recordings of conversations so that Amazon Connect has appropriate permissions to encrypt data sent to Kinesis. For more information about creating a customer master key (CMK) KMS key, see Creating Keys.

To enable agent event streams

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the console, choose the name in the Instance Alias column of the instance for which to enable agent event streams.
3. Choose Data streaming, then select Enable data streaming.
4. Under Agent Events, select the Kinesis stream to use, and then choose Save.

Sample Agent Event Stream

In the following agent event stream, the agent is assigned to a routing profile that requires them to take both chats and calls. They can take one call, and up to three chat at a time.

```json
{
    "AWSAccountId": "012345678901",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "Name": "Offline", // The agent is offline.
            "StartTimestamp": "2019-08-13T20:52:30.704Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "AgentEventStreamTest",
            "LastName": "Agent",
            "RoutingProfile": {
                "Concurrency": {
                    "AvailableSlots": 3, // This shows the agent has 3 slots available. They aren't on any chats right now.
                    "Channel": "CHAT",
                    "MaximumSlots": 3 // The agent's routing profile allows them to take up to 3 chats.
                },
                "DefaultOutboundQueue": {
                    "Channels": [
                        "VOICE" // This outbound queue only works for calls.
                    ]
                }
            }
        }
    }
}
```
"Name": "OutboundQueue"
},
"InboundQueues": [
{
  "Channels": [
    "VOICE",
    "CHAT"
  ],
  "Name": "null"  //This queue has a name of "null" because it's an agent queue, and agent queues don't have names.
},
{
  "Channels": [
    "CHAT",
    "VOICE"
  ],
  "Name": "Omni-channel-queue"  //This inbound queue takes both chats and calls.
}],
"Name": "AgentEventStreamProfile"
},
"Username": "aestest"
},
"Contacts": [ ]
},
"EventId": "EventId-1",
"EventTimestamp": "2019-08-13T20:58:44.031Z",
"EventType": "HEART_BEAT",
"PreviousAgentSnapshot": {
  "AgentStatus": {
    "Name": "Offline",
    "StartTimestamp": "2019-08-13T20:52:30.704Z"
  },
  "Configuration": {
    "AgentHierarchyGroups": null,
    "FirstName": "AgentEventStreamTest",
    "LastName": "Agent",
    "RoutingProfile": {
      "Concurrency": {
        "AvailableSlots": 3,
        "Channel": "CHAT",
        "MaximumSlots": 3
      },
      "AvailableSlots": 1,
      "Channel": "VOICE",
      "MaximumSlots": 1
    }
  },
  "DefaultOutboundQueue": {
    "Channels": [
      "VOICE"
Determine How Long an Agent Spends Doing ACW

There's no event in the agent event stream that tells you how long a contact is in the ACW state, and by extension how long an agent spends doing ACW. However, there's other data in the agent event stream that you can use to figure this out.

First, identify when the contact entered ACW. Here's how to do that:

1. Identify when the conversation between the contact and agent ENDED.
2. View the StateStartTimeStamp for the event.

For example, in the following agent event stream output, the contact enters ACW state at StateStartTimeStamp: "2019-05-25T18:55:55.017Z".

Tip
In the agent event stream, events are listed in reverse chronological order. We recommend reading through following examples by starting at the bottom of each example.

```json
{
  "AWSAccountId": "012345678901",
  "Channels": ["VOICE", "CHAT"],
  "Name": "Omni-channel-queue"
},
  "Channels": ["VOICE", "CHAT"],
  "Name": null
},
  "Channels": ["VOICE", "CHAT"],
  "Name": "Omni-channel-queue"
}
```

```json
{
  "Name": "AgentEventStreamProfile"
},
{ "Username": "aestest"
},
{ "Contacts": []
},
{ "Version": "2017-10-01"
}
```
"Name": "Available", //This just refers to the status that the agent sets manually in the CCP.
},
"Configuration": {
"AgentHierarchyGroups": null,
"FirstName": "(Removed)",
"LastName": "(Removed)",
"RoutingProfile": {
"DefaultOutboundQueue": {
"Name": "BasicQueue"
},
"InboundQueues": [
{
"Name": "BasicQueue"
},
{
"ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
"Name": "PrimaryQueue"
}
],
"Name": "Basic Routing Profile"
},
"Username": "(Removed)"
},
"Contacts": [
{
"Channel": "VOICE",
"ContactId": "ContactId-1", //This is the same contact the agent was working on when their state was CONNECTED (below).
Since it's still the same contact but they aren't connected, we know the contact is now in ACW state.
"InitialContactId": null,
"InitiationMethod": "OUTBOUND", //This indicates how the contact was initiated. OUTBOUND means the agent initiated contact with the customer.
INBOUND means the customer initiated contact with your center.
"Queue": {
"Name": "BasicQueue"
},
"QueueTimestamp": null,
"State": "ENDED", //This shows the conversation has ended.
"StateStartTimestamp": "2019-05-25T18:55:27.017Z" //This is the timestamp for the ENDED event (above),
which is when the contact entered ACW state.
}
],
"EventId": "EventId-1",
"EventType": "STATE_CHANGE", //This shows that the state of the contact has changed; above we can see the conversation ENDED.
"PreviousAgentSnapshot": {
"AgentStatus": {
"Name": "Available", //This just refers to the status that the agent sets manually in the CCP.

It means they were ready to handle contacts, not say, on Break.
},
"Configuration": {
  "AgentHierarchyGroups": null,
  "FirstName": "(Removed)",
  "LastName": "(Removed)",
  "RoutingProfile": {
    "DefaultOutboundQueue": {
      "Name": "BasicQueue"
    },
    "InboundQueues": [
        "Name": "BasicQueue"
      },
      { "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
        "Name": "PrimaryQueue"
      }
    ],
    "Name": "Basic Routing Profile"
  },
  "Username": "(Removed)"
},
"Contacts": [
  {
    "Channel": "VOICE", //This shows the agent and contact were talking on the phone.
    "ContactId": "ContactId-1", //This shows the agent was working with a contact identified as "ContactId-1".
    "InitialContactId": null,
    "InitiationMethod": "OUTBOUND",
    "Queue": {
      "Name": "BasicQueue"
    },
    "QueueTimestamp": null,
    "State": "CONNECTED", //This shows the contact was CONNECTED to the agent, instead of say, MISSED.
    "StateStartTimestamp": "2019-05-25T18:55:21.011Z" //This shows when the contact was connected to the agent.
  ]

Next, determine when a contact left ACW. Here’s how to do that:

1. Find where the CurrentAgentSnapshot has no contacts, and the state for the contact listed in the PreviousAgentSnapshot equals ENDED.
Determine How Long an Agent Spends Doing ACW

Because a `STATE_CHANGE` event also occurs when the agent’s configuration is changed, such as when they are assigned a different routing profile, this step confirms you have the right event.

2. Find where the `EventType` = "STATE_CHANGE".
3. View the `EventTimeStamp` for it.

For example, in the following agent event stream file, the contact left ACW at "EventTimestamp": "2019-05-25T18:55:32.022Z".

```json
{
   "AWSAccountId": "012345678901",
   "CurrentAgentSnapshot": {
      "AgentStatus": {
         "Name": "Available", //This just refers to the status that the agent sets manually in the CCP. It means they are ready to handle contacts, not say, on Break.
      },
      "Configuration": {
         "AgentHierarchyGroups": null,
         "FirstName": "(Removed)",
         "LastName": "(Removed)",
         "RoutingProfile": {
            "DefaultOutboundQueue": {
               "Name": "BasicQueue"
            },
            "InboundQueues": [
               {
                  "Name": "BasicQueue"
               },
               {
                  "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": [] //Since a contact isn’t listed here, it means ACW for ContactId-1 (below) is finished, and the agent is ready for a new contact to be routed to them.
   },
   "EventId": "477f2c4f-cdaa-4785-b1a8-97023dc1229d",
   "EventTimestamp": "2019-05-25T18:55:32.022Z", //Here's the EventTimestamp for the STATE_CHANGE event. This is when the contact left ACW.
   "EventType": "STATE_CHANGE", //Here's the STATE_CHANGE
   "PreviousAgentSnapshot": {
      "AgentStatus": {
```
"Name": "Available",  //This just refers to the status that the agent sets manually in the CCP.
It means they were at work, not say, on Break.
}
,"Configuration": { 
"AgentHierarchyGroups": null,
"FirstName": "(Removed)",
"LastName": "(Removed)",
"RoutingProfile": { 
"DefaultOutboundQueue": { 
"Name": "BasicQueue"
},
"InboundQueues": [
  {
  "Name": "BasicQueue"
  },
  {
  "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-PrimaryQueue",
  "Name": "PrimaryQueue"
  }
],  
"Name": "Basic Routing Profile"
},
"Username": "(Removed)"
},
"Contacts": [
  {
  "Channel": "VOICE",
  "ContactId": "ContactId-1",  //This is the ContactId of the customer the agent was working on previously.
  "InitialContactId": null,
  "InitiationMethod": "OUTBOUND",
  "Queue": { 
  "Name": "BasicQueue"
  },
  "QueueTimestamp": null,
  "State": "ENDED",  //The ACW for ContactId-1 has ended.
  }
],  
"Version": "2019-05-25"
}

Finally, to calculate the amount of time the contact was in the ACW state, and thus how long the agent spent working on it:

In this example, the agent spent 5.005 seconds doing ACW for ContactId-1.

Agent Event Streams Data Model

Agent event streams are created in JavaScript Object Notation (JSON) format. For each event type, a JSON blob is sent to the Kinesis data stream. The following event types are included in agent event streams:

- **LOGIN**—An agent login to the contact center.
- **LOGOUT**—An agent logout from the contact center.
- **STATE_CHANGE**—One of the following changed:
  - Something in the agent's configuration changed, such as their routing profile.
  - The agent changed their status in the CCP. For example, they changed it from Available to on Break.
  - The state of the conversation between then agent and contact changed. For example, they were connected and then 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. 158)
- **AgentSnapshot** (p. 159)
- **Configuration** (p. 160)
- **Contact Object** (p. 160)
- **HierarchyGroup Object** (p. 161)
- **AgentHierarchyGroups Object** (p. 162)
- **Queue Object** (p. 162)
- **RoutingProfile Object** (p. 162)

**AgentEvent**

The `AgentEvent` object includes the following properties:

**AgentARN**

The Amazon Resource Name (ARN) for the agent account.

Type: ARN

**AWSAccountld**

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.
Agent Event Streams Data Model

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 2019-05-25.

Type: String

**AgentSnapshot**

The AgentSnapshot object includes the following properties:

**AgentStatus**

Agent status data, including:

- **AgentARN**—the ARN for the agent.
- **Name**—this is the status of the agent that they manually set in the CCP. For example, their status might be Available, which means that they are ready for inbound contacts to be routed to them. Or it might be a custom status, such as Break or Training, which means that inbound contacts can't be routed to them BUT they can still make outbound calls.
- **StartTimestamp**—The 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.
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 InboundQueues 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 is added to each log in your contact flow as it 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:
   1. Select Enable to turn on logging for the flow.
   2. 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-f29a57b6e26",
  "ContactFlowId": "arn:aws:connect:us-east-2:0123456789012:instance/d-92673ef055/contact-flow/b1d791cf-1264-42e3-9a73-62cbcb3c9a45",
  "ContactFlowModuleType": "SetQueue",
  "Events": {
    "Queue": [
      "arn:aws:connect:us-east-2:670047220557:instance/d-92673ef044/queue/f030e43-9547-477c-b8ba-0bb7a72f7fa1"
    ]
  }
}
```

Tracking Customers Between Contact Flows

In many cases, customers interact with multiple contact flows in your contact center, being passed from one contact flow to another to appropriately assist them with their specific issue. Contact flow logs help
you track customers between different contact flows, by including the ID of the contact in each log entry. When a customer is transferred to a different contact flow, the ID for the contact associated with their interaction is included with the log for the new flow. You can query the logs for the contact ID to trace the customer interaction through each contact flow. In larger, high-volume contact centers, there can be multiple streams for contact flow logs. If a contact is transferred to a different contact flow, the log may be in a different stream. To make sure that you are finding all of the log data for a specific contact, you should search for the contact ID in the entire CloudWatch log group instead of in a specific log stream.

Create Alerts for Contact Flow Log Events

You can configure CloudWatch to define a filter pattern that looks for specific events in your contact flow logs and then creates an alert when an entry for that event is added to the log. For example, you can set an alert for when a contact flow block goes down an error path as a customer interacts with the flow. Log entries are typically available in CloudWatch within a short time, giving you near real-time notification of events in contact flows.

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

Dimension:

- **InstanceId**: The ID of your instance
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

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: ContactFlow
- **ContactFlowName**: The name of your contact flow

CallRecordingUploadError

The number of call recordings that failed to upload to the Amazon S3 bucket configured for your instance. This is the bucket specified in Data Storage > Call Recordings settings for the instance.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: CallRecordings

CallsPerInterval

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

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: VoiceCalls

ConcurrentCalls

The number of concurrent active voice calls in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active calls at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active voice calls are included, not only active calls that are connected to agents.

While all statistics are available in CloudWatch for concurrent voice calls you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: VoiceCalls

ConcurrentCallsPercentage

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

Unit: Percent

Dimensions:
- **InstanceId**: The ID of your instance
• **MetricGroup: VoiceCalls**

**ContactFlowErrors**

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

Unit: Count

Dimensions:

• **InstanceId**: The ID of your instance
• **MetricGroup**: ContactFlow
• **ContactFlowName**: The name of your contact flow

**ContactFlowFatalErrors**

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

Unit: Count

Dimensions:

• **InstanceId**: The ID of your instance
• **MetricGroup**: ContactFlow
• **ContactFlowName**: The name of your contact flow

**LongestQueueWaitTime**

The longest amount of time, in seconds, that a contact waited in a queue. This is the length of time a contact waited in a queue during the refresh interval selected in the CloudWatch dashboard, such as 1 minute or 5 minutes.

Unit: Seconds

Dimensions:

• **InstanceId**: The ID of your instance
• **MetricGroup**: Queue
• **QueueName**: The name of your queue

**MissedCalls**

The number of voice calls that were missed by agents during the refresh interval selected, such as 1 minute or 5 minutes. A missed call is one that is not answered by an agent within 20 seconds.

To monitor the total missed calls in a given time period, take a look at the Sum statistic in CloudWatch.

Unit: Seconds

Dimensions:

• **InstanceId**: The ID of your instance
• **MetricGroup**: VoiceCalls

**MisconfiguredPhoneNumbers**

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

Unit: Count

Dimensions:

• **InstanceId**: The ID of your instance
• **MetricGroup**: VoiceCalls
PublicSigningKeyUsage

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

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **SigningKeyId**: The ID of your signing key

QueueCapacityExceededError

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

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: Queue
- **QueueName**: The name of your queue

QueueSize

The number of contacts in the queue. The value reflects the number of contacts in the queue at the time the dashboard is accessed, not for the duration of the reporting interval.

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: Queue
- **QueueName**: The name of your queue

ThrottledCalls

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

To monitor the total throttled calls in a given time period, take a look at the Sum statistic in CloudWatch.

Unit: Seconds

Unit: Count

Dimensions:
- **InstanceId**: The ID of your instance
- **MetricGroup**: VoiceCalls

ToInstancePacketLossRate

The ratio of packet loss for calls in the instance, reported every 10 seconds. Each data point is between 0 and 1, which represents the ratio of packets lost for the instance.

Unit: Percent

Dimensions:
- **Participant**: Agent
• Type of Connection: WebRTC
• Instance ID: The ID of your instance
• Stream Type: Voice

Amazon Connect CloudWatch Metrics Dimensions

In CloudWatch, a dimension is a name/value pair that uniquely identifies a metric. In the dashboard, metrics are grouped by dimension. The following dimensions are used in the CloudWatch dashboard for Amazon Connect metrics. When you view metrics in the dashboard, only metrics with data are displayed. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard. The following dimensions are used for Amazon Connect metrics in CloudWatch.

Contact Flow Metrics Dimension

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
• CallsPerInterval
• 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

Note
If a queue has a dimension name in non-ASCII characters, you won’t be able to see it in CloudWatch.

Filters metric data by queue. Includes the following metrics:
• CallBackNotDialableNumber
• LongestQueueWaitTime
• QueueCapacityExceededError
• QueueSize
Amazon Connect Metrics and Contact Trace Records

In Amazon Connect, about contacts are captured in contact trace records (CTR). This data can include the amount of time a contact spends in each state: customer on hold, customer in queue, agent interaction time. The basis for most historical and real-time metrics in Amazon Connect is the data in the CTR. When you create metrics reports, the values displayed for most 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 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 about the activity of agents in your contact center, you can use Amazon Connect Agent Event Streams (p. 150).

Contents
- What's New in Metrics (p. 171)
- About Agent Status (p. 174)
- About Contact States (p. 175)
- Real-time Metrics Reports (p. 177)
- Historical Metrics Reports (p. 186)
- Contact Search (p. 199)
- View a CTR in the UI (p. 199)
- Contact Trace Records Data Model (p. 200)

What's New in Metrics

Thanks to your feedback, we’ve made changes to Amazon Connect metrics. This topic gives you a overview of the improvements.

Real-Time Metrics: Name Changes for "Missed" and "Agent Status" and "On Call"

The following metrics were renamed:

<table>
<thead>
<tr>
<th>Old Name</th>
<th>New Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed</td>
<td>Agent non-response</td>
</tr>
</tbody>
</table>
Label Updates for "Agent Activity" and "Contact State"

<table>
<thead>
<tr>
<th>Old Name</th>
<th>New Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Status</td>
<td>Agent Activity</td>
</tr>
<tr>
<td>On Call</td>
<td>On Contact</td>
</tr>
</tbody>
</table>

For each metric, existing saved reports automatically start displaying the new name; you don't need to do anything for the new name to appear in your reports.

The column order for a saved report containing one of these metrics stays the same. For example, if you previously saved a report where Agent Status was the third metric, now when you open that saved report, Agent Activity is the name for the third metric.

For Missed, only the name of the metric changed; the underlying calculation stayed the same. We've changing the name of this metric to Agent non-response so it better reflects its definition:

- **Agent non-response** increments whenever a contact is offered to an agent, and the agent doesn't respond to the contact for whatever reason.

  For example, the agent could have intentionally let the timer run out, or the agent could have forgotten to grant microphone access in the Contact Control Panel and never heard the ring. In these situations, Amazon Connect doesn't drop the contact. Instead, the routing engine will offer it to another available agent, while the customer continues to wait in queue. This means a single contact could result in multiple Agent non-responses before an agent responds and handles the contact.

For On Call, the name change to On Contact applies to the Real-time metrics UI only. You can continue using AGENTS_ON_CALL with the GetCurrentMetricData API to retrieve data for this metric.

### Label Updates for "Agent Activity" and "Contact State"

Labels are the values returned in a report. For example, in the following image Available and Basic Routing Profile are labels.

For **Agent Activity** and **Contact State**, we renamed some of the labels that describe what the agent's current activity is and what's happening with the contact they are currently working on. This way, the labels in the Real-Time Metrics report are more consistent with the labels the agent sees in the Contact Control Panel. They also align with the data returned about these different states in other parts of Amazon Connect.

When the name of Agent Status changed to Agent Activity, the following labels changed, too:
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Before: Agent Status Labels</th>
<th>After: Agent Activity Labels</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent is logged in but offline</td>
<td>Not shown</td>
<td>Not shown</td>
<td></td>
</tr>
<tr>
<td>Agent switches to <strong>Available</strong> in the CCP</td>
<td>Available</td>
<td>Available</td>
<td></td>
</tr>
<tr>
<td>Agent has an incoming call</td>
<td>CallIncoming</td>
<td>Incoming</td>
<td><strong>ContactState</strong> = <strong>Incoming contact</strong></td>
</tr>
<tr>
<td>Agent has an incoming callback</td>
<td>CallbackIncoming</td>
<td>Incoming</td>
<td><strong>ContactState</strong> = <strong>Incoming</strong></td>
</tr>
<tr>
<td>Agent accepted a callback, which is now making an outbound call to the customer</td>
<td>Calling</td>
<td>On Contact</td>
<td><strong>ContactState</strong> = <strong>Outbound callback</strong></td>
</tr>
<tr>
<td>Agent makes outbound call (regardless of what status the agent chose in their CCP)</td>
<td>Calling</td>
<td>On Contact</td>
<td><strong>ContactState</strong> = <strong>Outbound contact</strong></td>
</tr>
<tr>
<td>Agent missed a phone call due to timer expired</td>
<td>MissedCallAgent</td>
<td>Missed</td>
<td></td>
</tr>
<tr>
<td>Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
<tr>
<td>Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
<tr>
<td>After agent hangs up call</td>
<td>After call work</td>
<td>After contact work</td>
<td></td>
</tr>
<tr>
<td>Agent is on Lunch (a custom status)</td>
<td>Lunch</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>Supervisor's activity state if they are monitoring some agent</td>
<td>Monitoring</td>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Agent's activity state if they are connected to customer while being monitored by a supervisor</td>
<td>On call</td>
<td>On Contact</td>
<td></td>
</tr>
</tbody>
</table>
The following table shows the how the labels changed for Contact State.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Label Name Before</th>
<th>Label Name After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent is logged in but offline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent switches to <strong>Available</strong> in the CCP</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Agent has an incoming call</td>
<td>-</td>
<td><strong>Incoming contact</strong></td>
</tr>
<tr>
<td>Agent has an incoming callback</td>
<td>-</td>
<td><strong>Inbound callback</strong></td>
</tr>
<tr>
<td>Agent accepted a callback, which is now making an outbound call to the customer</td>
<td>Initial</td>
<td><strong>Outbound callback</strong></td>
</tr>
<tr>
<td>Agent makes outbound call (regardless of what status the agent chose in their CCP)</td>
<td>Initial</td>
<td><strong>Outbound contact</strong></td>
</tr>
<tr>
<td>Agent missed a phone call due to timer expired</td>
<td>Missed call</td>
<td><strong>Missed contact</strong></td>
</tr>
<tr>
<td>Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)</td>
<td>Busy</td>
<td><strong>Connected</strong></td>
</tr>
<tr>
<td>Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)</td>
<td>OnHold</td>
<td><strong>On hold</strong></td>
</tr>
<tr>
<td>After agent hangs up call</td>
<td>After call work</td>
<td><strong>After contact work</strong></td>
</tr>
<tr>
<td>Agent is on Lunch (a custom status)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Supervisor's contact state if they are monitoring an agent</td>
<td>Monitoring</td>
<td><strong>Monitoring</strong></td>
</tr>
</tbody>
</table>

About Agent Status

Agents have a status. It's manually set in the Contact Control Panel (CCP).

- When they're ready to handle contacts, they set their status in the CCP to **Available**. This means inbound contacts can be routed to them.
- When agents want to stop taking inbound contacts, they set their status to a custom status that you create, such as **Break** or **Training**. They can also change their status to **Offline**.

It's possible for agents to make outbound calls when their status in the CCP is set to a custom status. Technically, agents can make an outbound call when their CCP is set to **Offline**.

For example, an agent wants to make an outbound call to a contact. Because they don't want contacts to be routed to them during this time, they set their status to a custom status. So when you look at your
metrics, you'll see the agent is simultaneously on NPT (the metric that indicates a custom status) and On Call, for example.

**About ACW (After Contact Work)**

After a conversation between an agent and customer ends, the contact is moved into the ACW state, not the agent. The agent's status in the CCP is still set to Available.

When the agent finishes doing ACW for the contact, they click Clear to clear that slot so another contact can be routed to them.

Because we're tracking the contact state, if you want to identify how long an agent spent on ACW for a contact:

- In the historical metrics report, After contact work time captures the amount of time each contact spent in ACW.
- In the agent event stream, you have to do some calculations. For more information, see Determine How Long an Agent Spends Doing ACW (p. 153).

**How Do You Know When an Agent Can Handle Another Contact?**

The Availability metric tells you when agents are finished with a contact and ready to have another one routed to them.

**What Appears in the Real-Time Metrics Report?**

To find out what the agent status is in the real-time metrics report, look at the Status metric.

**What Appears in the Agent Event Stream?**

In the agent event stream you'll see the AgentStatus, for example:

```json
{
  "AWSAccountId": "012345678901",
  "CurrentAgentSnapshot": {
    "AgentStatus": {
      "Name": "Available", //When an agent sets their status to "Available" it means they are ready for inbound contacts to be routed to them, and not say, at Lunch.
    }
  }
}
```

**About Contact States**

Contact states appear in two places: the real-time metrics reports and the agent event stream.
Contact States in the Agent Event Stream

There are different events that can appear in the lifecycle of a contact. Each of these events appear in the agent event stream as a State. A contact can have the following states that appear in the agent event stream:

- **INCOMING** - This is specific to queued callbacks. The agent is presented with a callback.
- **PENDING** - This is specific to queued callbacks.
- **CONNECTING** - The agent has accepted the contact. Now the contact object is being connected to the customer.
- **CONNECTED** - They are in a conversation with the agent.
- **CONNECTED_ONHOLD** - They are in a conversation with the agent, and the agent has put the customer on hold.
- **MISSED** - The contact was missed by the agent.
- **ERROR** - This appears when, for example, the customer abandons the call during outbound whisper.
- **ENDED** - The conversation has ended, and the agent has started doing ACW for that contact.

Here's what the contact state looks like in the agent event stream:

```
"Contacts": [  
  {  
    "Channel": "VOICE",  //This shows the agent and contact were talking on the phone.
    "ContactId": "ContactId-1",  //This shows the agent was working with a contact identified as "ContactId-1".
    "InitialContactId": null,
    "InitiationMethod": "OUTBOUND",  //This shows the agent reached the customer by making an outbound call.
    "Queue": {  
    },
    "QueueTimestamp": null,
    "State": "CONNECTED",  //Here's the contact state. In this case, it shows the contact was CONNECTED to the agent, instead of say, MISSED.
    "StateStartTimestamp": "2019-05-25T18:55:21.011Z"  //This shows when the contact was connected to the agent.
  }  
]
```

Events in the Contact Trace Record (CTR)

A contact trace record (CTR) captures events associated with the contact in your contact center. For example, how long the contact lasted, when it started and stopped. For a list of all data that's captured in the CTR, see Contact Trace Records Data Model (p. 200).

A CTR is opened for a customer when they are connected to your contact center. The CTR is completed when the interaction with the contact flow or agent ends. This means it's possible for a customer to have multiple CTRs.

The following diagram shows when a CTR is created for a contact.
Each time a contact is connected to an agent, a new CTR is created. The CTRs for a contact are linked together through the contactId fields: original, next, and previous.

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.

Contents
- How Often Real-Time Metrics Refresh (p. 178)
- Create a Real-time Metrics Report (p. 178)
How Often Real-Time Metrics Refresh

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

- The **Real-time metrics** page refreshes every 15 seconds, as long as the page is active. For example, if you have multiple tabs open in your browser and navigate to a different tab, the real-time metric page won't be updated until you return to it.
- Metrics such as **Active** and **Availability** refresh as activity occurs, with a small system delay for processing the activity.
- Agent near real-time metrics, such as **Missed** and **Occupancy**, refresh every 5 minutes.
- Contact near real-time metrics refresh about a minute after a contact ends.

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 Assign Permissions: Security Profiles (p. 136).

**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:
No Metrics or Too Few Rows in a Queues Report?

It's possible to run a manually configured queues report and have no metrics returned, or fewer rows than expected.

This is because a queues report only includes data for a maximum of 100 queues, using one row per queue. If a queue doesn't have any activity* during the time range for the report, it's excluded from the report rather than included with null values. This means that if you create a report, and there is no activity for any of the queues included in the report, your report will not include any data.

This applies to the GetCurrentMetricsData API as well. This means that if a queue is not considered active, if you query for its metrics using the API you won't get any data.

Tip
*Here's how we define whether a queue is active: there's at least one contact in queue or there's at least one online agent for that queue. Otherwise, it's considered inactive.

In the following situations, you could end up with no metrics or fewer rows than expected:

1. You're attempting to run a report with no filters or groupings, and have more than 100 queues in your instance. The report pulls metrics for the first 100 queues, and then displays only those that are active.

2. You're attempting to run a report with filters and groupings, but it still has more than 100 queues matching that criteria. To process this request, Amazon Connect applies all the specified filters and groupings. This pulls the first 100 queues matching that criteria. Then out of those queues, it displays only the active ones.

   For example, let's say you have 300 queues in your instance. Of these, 200 match your criteria; 100 are active and by coincidence all happen to be Queues #100-#200. When you run the report, you'd get just 1 row (Queue #100) since the other 99 queues that were returned (Queues #1-#99) were considered inactive and were not displayed.

3. You're running a report with fewer than 100 queues. While you may expect to see metrics for all filtered queues, only active queues are shown on the real-time metrics report page. Try changing the settings for the report, such as changing the time range.
2. Click Settings.

3. On the Groupings tab, choose Queues grouped by routing profiles.
4. Choose Apply.

List Agents Grouped By Routing Profile

1. Go to Metrics and quality, Real-time metrics, Queues.
2. Choose New table, Agents.
3. Click Settings.

4. On the Filters tab, choose Routing profiles. In Include, select the routing profiles you want included in the table.

5. Choose Apply.

View How Many Customers Are Waiting In Queue

To see the number of customers waiting in queue

1. Go to Metrics and quality, Real-time metrics, Queues.
2. By default, customers who are waiting for a call back are counted in the In queue column. This column counts all customers who are in a queue for an agent, not just the callback customers.
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. When you create a customized real-time metrics report, to include this metric, choose a Queues report for the type. On the Filters tab, choose Queues, then on the Metrics tab you'll have the option to include Abandoned.

Active

Count of active slots. This number is incremented for each contact where the contact state is either Connected, On Hold, After contact work, or Outbound ring.

ACW

Count of contacts who are in an AfterContactWork state.

Agent Activity

If an agent is handling a single contact, this metric may have the following values: Available, Incoming, On contact, Rejected, Missed, Error, After contact work, or a custom status.

If an agent is handling concurrent contacts, Amazon Connect uses the following logic to determine the state:

- If at least one contact is in Error, Agent Activity = Error.
- Else if at least one contact is Missed contact, Agent Activity = Missed.
- Else if at least one contact is Rejected contact, Agent Activity = Rejected.
- Else if at least one contact is Connected, On Hold, After contact work, or Outbound callback, Agent Activity = On contact.
- Else if at least one contact is After contact work, Agent Activity = After Contact Work.
- Else if at least one contact is Incoming/Inbound Callback, Agent Activity = Incoming.
- Else if agent status is a custom status, Agent Activity is the custom status.
• Else if agent status is Available, Agent Activity = Available.

If a supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, then the supervisor’s Agent Activity will display as Monitoring. The Agent Activity of the agent who is being monitored is still On Contact.

Agent First Name

The first name of the agent, as entered in their Amazon Connect user account.

Agent Hierarchy

The hierarchy the agent is assigned to, if any.

Agent hung up

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

Agent Last Name

The last name of the agent, as entered in their Amazon Connect user account.

Agent Name

The name of the agent, displayed as follows: Agent Last Name, Agent First Name.

Agent non-response

Count of contacts routed to an agent but not answered by that agent, including contacts abandoned by the customer.

If a contact is not answered by a given agent, we attempt to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times (including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

This metric was previously named Missed.

AHT (Average Handled Time)

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 conversation ending.

API contacts handled

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

Availability

For each agent, the number of available slots they have that can be routed contacts.

The number of available slots for an agent are based on their routing profile (p. 42). For example, let’s say an agent’s routing profile specifies they can handle either one voice contact or up to three chat contacts simultaneously. If they are currently handling one chat, they have two available slots left, not three.

What causes this number to go down? A slot is considered unavailable when:

• A contact in the slot is: connected to the agent, in After Contact Work, inbound ringing, outbound ringing, missed, or in an error state.
• A contact in the slot is connected to the agent and on hold.

Amazon Connect doesn’t count an agent’s slots when:
The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.

The agent can't take contacts from that channel per their routing profile.

Available

The number of agents who can take an inbound contact. An agent can only take inbound contacts when they manually set their status to Available in the CCP (or in some cases when their supervisor changes it).

This is different from how many more inbound contacts an agent could take. If you want to know how many more contacts an agent can have routed to them, look at the Availability metric. It indicates how many slots the agent has free.

What causes this number to go down? An agent is considered **unavailable** when:

- The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.
- The agent is at maximum capacity. For example, they are only allowed to handle 3 contacts at a time and they are currently handling 3.
- The agent has a contact in a missed or error state, which prevents the agent from taking any more contacts until they are flipped back to routable.

Avg abandon time

Average time, in seconds, that abandoned contacts were in the queue before being abandoned.

Avg ACW

Average time, in seconds, that contacts spent in the **After contact work** state, during the specified time range.

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.

Capacity

Displays the maximum capacity that's set in the routing profile currently assigned to the agent. This column can be filtered by channel.
If an agent’s routing profile is configured to handle either one voice or up to three chats, then their maximum capacity equals three, when not filtered by channel.

**Consult**

Count of contacts in the queue that were handled by an agent, and the agent consulted with another agent or a call center manager during the contact.

**Contact State**

The state of the contacts the agent is currently handling. The state can be: Connected, On Hold, After contact work, Incoming, Calling, or Missed contact.

For queued callbacks, the contact state can also Callback incoming or Callback dialing.

If a supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, the supervisor’s contact state is Monitoring; the agent’s contact state is Connected.

**Duration**

Amount of time that the agent has been in the current Agent Activity State.

**Error**

When this term appears in the Agent Status column, it means there’s a contact in an error state.

**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.

**NPT (Non-Productive Time)**

Count of agents who have set their status in the CCP to a custom status. That is, their CCP status is other than Available or Offline.

**Tip**

Agents can handle contacts while their CCP status is set to a custom status. For example, agents can be On call or doing ACW for a contact while their CCP is set to a custom status. This means it’s possible for agents to be counted as On call and NPT at the same time.

**Occupancy**

Percentage of time that agents was active on contacts. This percentage is calculated as follows:
(Agent Handle Time / (Agent Handle Time + Agent Idle Time)) * 100

**Important**

*Occupancy* doesn't account for concurrency. That is, an agent is considered 100% occupied for a given interval if they are handling at least one contact for that entire duration.

**Oldest**

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

**On contact**

Count of agents currently on a contact. An agent is "on a contact" when they are handling at least one contact who is either connected, on hold, in After contact work, or outbound ring.

**Online**

Count of agents who have set their status in the CCP to something other than **Offline**. For example, they may have set their status to Available, or to a custom value such as Break or Training.

The Online metric doesn't tell you how many agents can be routed contacts. For that metric, see **Available** (p. 183).

This metric can be confusing so let's look at an example. Say you see this in a Queues report:

- Online = 30
- On Call = 1
- NPT = 30
- ACW = 0
- Error = 0
- Available = 0

This means 30 agents have set their status in the CCP to a custom status. 1 of those 30 agents is currently on a contact.

**Queue**

The name of the queue associated with the contact the agent is currently handling.

**Queued**

Count of contacts added to the queue during the specified time range.

**Routing Profile**

The routing profile for the agent.

**Scheduled**

Count of customers in the queue for which there is a callback scheduled.

**SL X**

Percentage of contacts removed from the queue between 0 and X seconds after being added to it (Service Level). A contact is removed from the queue when one of the following occurs: an agent answers the call, the customer abandons the call, or the customer requests a call back. The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

**Staffed**

Count of agents who are online in the CCP, and not in NPT (a custom status).

Another way of thinking about this is, there are two scenarios in which **Staffed** is not incremented:

- The agent's status in the CCP is set to **Offline**.
The agent's status in the CCP is set to a custom status.

For example, let's say an agent sets their status in the CCP to a custom status such as Break and they make an outbound call. Now the agent is On call, but Staffed is 0.

If the agent sets their status in the CCP to Available and makes an outbound call, the agent is On call and Staffed is 1.

This metric is available on the Queues report.

**Status**

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

**Transferred in**

Count of contacts transferred into the queue during the specified time range.

**Transferred in from queue**

Count of contacts transferred into the queue from another queue during a Customer queue flow.

**Transferred out**

Count of contacts transferred out of the queue during the specified time range.

**Transferred out from queue**

Count of contacts transferred out of the queue to another queue during a Customer queue flow.

---

**Historical Metrics Reports**

Historical metrics reports include data about past, completed activity and performance in your contact center. Amazon Connect includes built-in historical reports that you can start using right away. You can also build your own custom reports.

When creating and analyzing your historical metrics reports, keep in mind that there are two categories of metrics:

**CTR-driven metrics**

These metrics are based on formed CTR records. For a given interval, CTRs whose disconnect date falls in the interval are selected to calculate metrics. For example, if a contact starts at 05:23 and ends at 06:15, this contact contributes 52 minutes of metrics for the 06:00-06:30 interval.

Example CTR-driven metrics are Service level, Agent interaction time, and After contact work time.

**Agent activity-driven metrics**

These metrics are based on agent activities, like agent status changes, agent conversation changes. The metrics reflect on the actual time the activity happens. For example, if agent handles a contact from 05:23 to 06:15, the Agent on contact time has 7 minutes for the 05:00-05:30 interval, 30 minutes for the 05:30-06:00 interval, and 15 minutes for the 06:00-06:30 interval.

Example agent activity-driven metrics are Agent on contact time, Agent idle time, and Non-Productive Time.

You can customize the report settings to get the view of the data that is most meaningful for your organization. You can change the time frame for the report, which metrics are included in the report,
and how data is grouped in the report. After you have customized a report, you can save it for future reference. You can generate a report using a recurring schedule that you define.

Contents
- Create a Historical Metrics Report (p. 187)
- Report Limits (p. 189)
- Schedule a Historical Metrics Report (p. 189)
- Update a Historical Metrics Report (p. 190)
- Download a Historical Metrics Report (p. 191)
- Historical Metrics Definitions (p. 191)

Create a Historical Metrics Report

Although Amazon Connect includes built-in historical reports, you can create your own custom reports so you look at only the data that's of interest to your organization.

Requirement
- You must have permission to access metric data. The following security profiles include this permission: CallCenterManager and QualityAnalyst. For more information, see Assign Permissions: Security Profiles (p. 136).

Grouping Options

You can group the metrics included in your reports in different ways to provide greater insight into how your contact center is performing.

You can group reports by queue, agent, agent hierarchy, routing profile, or phone number. The metric calculations, and therefore metrics values displayed in the report, are different when reports are grouped differently. For example, if you group a report by queue, the value of a metric includes all contacts associated with the queue. If you group a report by agent, the values for the metrics associated with queues might not provide much insight.

When you create a report, the values for calculated metrics are displayed as rows in the report. The rows in the report are grouped by the grouping options you select. Grouping the data enables you to generate global data for your contact center, or more specific data for queues, agents, routing profiles, or agent hierarchy defined in your contact center.

For example, consider the Contacts handled metric. This metric is a count of the contacts handled during the time range defined for the report. Here are the results based on the grouping:

- **Queue** - The metric is the total number of contacts handled during the time range from that queue by all agents in your contact center.
- **Agent** - The metric is the total number of contacts handled by that agent during the time range across all queues and routing profiles.
- **Routing Profile** - The metric is the total number of contacts handled during the time range by agents assigned that routing profile.
- **Queue, then Agent, then Routing Profile** - The metric is the total number of contacts that agent assigned that routing profile handled from that queue.

Agent activity can be included in one routing profile at a time, but agents can switch between routing profiles over the reporting time interval. If agents are assigned multiple routing profiles and handle
contacts from multiple queues, there are multiple rows in the report for each routing profile assigned to
the agent and the queue that the agent handled contacts from.

Filters

When you customize a report, you can add filters to control which data is included in the report. You can
filter on the following:

- **Queue**—Includes data only for the specified queues. If you don't specify any queues, all queues are
  included.

- **Routing profile**—Includes data only for the agents assigned to the specified routing profiles. If you
don't specify any routing profiles, data for all agents for all routing profiles is included.

- **Agent hierarchy**—Includes data only for the contacts handled by agents in the specified hierarchies.
  If you don't specify a hierarchy, data for all contacts handled by agents in all hierarchies is included.
  When only one hierarchy is specified, you can specify a more granular filter within the hierarchy.

- **Phone number**—Includes data only for the contacts associated with the specified phone numbers. If
  you don't specify a phone number, data for all contacts associated with all phone numbers is included.

How to Create a Historical Metrics Report

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose **Metrics and quality, Historical metrics**.
3. Choose one of the following report types, which group and order the data in different ways, and
   include different metrics:
   - **Queues**
     - **Contact metrics**
     - **Agent metrics**
   - **Agents**
     - **Agent performance**
   - **Phone numbers**
     - **Contact metrics**
4. To customize your report, choose the gear icon.
5. On the **Interval & Time range** tab, do the following:
   a. For **Interval**, choose **30 minutes** to get a row for each 30-minute period in the time range, **Daily** to get a row for each day in the time range, or **Total** to get all data for the time range in a single row.
   b. For **Time Zone**, select a time zone, which determines the hour at which a day starts. For example, to align the report with your calendar days, select the time zone for your location.

You should use the same time zone for reports over time to get accurate and consistent metrics data for your contact center. Using different time zones for different reports may result in different data for the same time range selection.

   c. The possible values for **Time range** depend on the value that you select for **Interval**. Alternatively, you can specify a custom time range.

      For **Last x days** and **Month to date**, the current day is not included in the report. **Yesterday** specifies the previous calendar day while **Last 24 hours** specifies the 24 hours prior to the current time.

6. (Optional) On the **Groupings** tab, choose up to five groupings. If you choose one grouping option,
   the data is grouped by that option. If you choose multiple grouping options, the data is group by
the first grouping option and then by the subsequent grouping options. For more information, see Grouping Options (p. 187).

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. 188).

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. 191).

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.

Report Limits

Historical metrics reports have the following limits:

Data only for active queues

- You can get data only for active queues. A queue is inactive if there are no contacts in the queue and no agents available.

80k Cell Limit

There is currently an 80k cell limitation on historical metrics reports and scheduled reports. This applies to the total number of cells (columns * rows), accounting for grouping and filtering.

For example, let's say you create a historical metrics report with this criteria:

- Grouped by agents
- With an interval of 30 minutes
- For the last 24 hours
- Limited to include only 5 metrics
- Filtered to show only contacts handled in BasicQueue

If only 10 agents handled contacts in BasicQueue during this time, then you would expect to see (24*2)*5*10 = 2400 cells that count towards the 80k limit.

A message informs you if you reach the limit.

Schedule a Historical Metrics Report

Before you schedule a historical metrics report, here are a few things you need to know:

Others Can Access the Report

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

Scheduled Reports are Located in an Amazon S3 Bucket

- Scheduled reports are saved as CSV files in the Amazon S3 bucket specified for reports for your contact center. When you set up the scheduled report, you can add a prefix to the location in Amazon S3 for the report files.
When the report is exported to your Amazon S3 bucket, the file name includes the date and UTC time when the report was created. The Last modified date for the file is displayed using the time zone for the Amazon S3 bucket, and may not match the creation time for the report, which is in UTC.

There's a 15 Minute Delay

- For scheduled reports, there is a delay of 15 minutes after the scheduled report time before the report is generated. This is to ensure that the report includes the data for all of the activity that occurred during the time range specified for the report. Data from your contact center is not immediately processed and available to include in reports, so some data from the time range might not be captured in a report if the report is generated at the second the time range ends.
- For example, if you create a scheduled report for time frame of 8:00 AM to 5:00 PM, and there is activity in your contact center between 4:46:00 PM and 4:59:59 PM, the data about that activity may not be aggregated prior 5:00 PM when the report is scheduled to generate. Instead, the report is generated after 5:15 PM, by which time the data for the last 15 minutes of the time range is included in the report.

A Scheduled Yesterday Report Works Like a Last 24 Hours Report

- Usually Yesterday specifies the previous calendar day while Last 24 hours specifies the 24 hours prior to the current time. However, if you schedule to run a Yesterday report, it will work like a Last 24 hours report.

No Message if a Scheduled Report Doesn't Run

- If a scheduled report fails to run, you won't get any message in the Amazon Connect UI. You just won't see the report in the Amazon S3 location.

How to Schedule a Historical Metrics Report

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Create a new report and save it, or open a saved report.
3. Choose the down arrow next to Save in the top-right corner of the page and choose Schedule.
4. On the Recurrence tab, specify how often this report should be run (for example, weekly on Saturdays) and the range (for example, from midnight for the previous 5 days).
5. (Optional) On the Delivery Options tab, specify a prefix for the location in Amazon S3 for the report files.
6. Choose Create.

Update a Historical Metrics Report

After you save a report, you can update it at any time.

To update a historical metrics report

1. Log in to your contact center using your access URL (https://domain.awsapps.com/connect/login).
2. Choose Metrics and quality, Saved reports.
3. From the Historical metrics tab, choose the name of the report. Choose the gear icon, update the report settings as needed, and choose Apply.
4. To update the current report, choose Save. To save your changes to a new report, choose Save as.
Download a Historical Metrics Report

You can download the data included in a report as a comma-separated value (CSV) file so you can use it with other applications. If there's no data for one of the selected metrics, the field in the downloaded CSV file contains a dash.

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

The total time that an agent spent doing ACW for a contact.

You specify the amount of time an agent has to do ACW in their agent configuration settings (p. 45). When a conversation with a contact ends, the agent is automatically allocated to do ACW for the contact. They stop doing ACW for a contact when they indicate they are ready for another contact in the CCP.

Type: String (hh:mm:ss)

Category: CTR-driven metric

Agent answer rate

Percentage of contacts routed to an agent that were answered.

Type: String

Min value: 0.00%

Max value: 100.00%

Category: Agent activity-driven metric

Agent first name

The first name of the agent, as entered in their Amazon Connect user account. This metric is available only when grouping by agent.

Type: String

Length: 1-255

Agent idle time

After the agent sets their status in the CCP to Available, this is the amount of time they weren't handling contacts + any time their contacts were in an Error state.

Agent idle time doesn't include the amount of time from when Amazon Connect starts routing the contact to the agent, to when agent picks up or declines the contact.
Agent interaction and hold time

Sum of Agent interaction time (p. 192) and Customer hold time (p. 198).

Type: String (hh:mm:ss)

Category: CTR-driven metric

Agent interaction time

Total time that agents spent interacting with customers on a contact. This does not include Customer Hold Time (p. 198) or After Contact Work Time (p. 191).

Type: String (hh:mm:ss)

Category: CTR-driven metric

Agent last name

The last name of the agent, as entered in their Amazon Connect user account. This metric is available only when grouping by agent.

Type: String

Length: 1-255

Agent name

The name of the agent, displayed as follows: Agent last name, Agent first name. This metric is available only when grouping by agent.

Agent non-response

Count of contacts routed to an agent but not answered by that agent, including contacts abandoned by the customer.

If a contact is not answered by a given agent, we attempt to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times (including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

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

Type: Integer

Category: Agent activity-driven metric

Agent on contact time

Total time that an agent spent on a contact, including Customer Hold Time (p. 198) and After Contact Work Time (p. 191). This does not include time spent on a contact while in a custom status.

Tip
If you want to include the time spent in a custom status, see Contact handle time (p. 194).

Type: String (hh:mm:ss)

Category: Agent activity-driven metric
API contacts

Count of contacts that were initiated using an Amazon Connect API operation, such as StartOutboundVoiceContact. This includes contacts that were not handled by an agent.

Type: Integer

Category: CTR-driven metric

API contacts handled

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

Type: Integer

Category: CTR-driven metric

Average after contact work time

Average amount of time that an agent spent doing After Contact Work (ACW) for contacts. This is calculated by averaging AfterContactWorkDuration (p. 201) (from the CTR) for all contacts included in the report, based on the selected filters.

Type: String (hh:mm:ss)

Category: CTR-driven metric

Average agent interaction and customer hold time

Average of the sum of the agent interaction and customer hold time. This is calculated by averaging the sum of the following values from the CTR: AgentInteractionDuration (p. 201) and CustomerHoldDuration (p. 201).

Type: String (hh:mm:ss)

Category: CTR-driven metric

Average agent interaction time

Average time that agents interacted with customers during contacts.

Type: String (hh:mm:ss)

Category: CTR-driven metric

Average customer hold time

Average time that customers spent on hold while connected to an agent. This is calculated by averaging CustomerHoldDuration (p. 201) (from the CTR).

Type: String (hh:mm:ss)

Category: CTR-driven metric

Average handle time

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

Type: String (hh:mm:ss)

Category: CTR-driven metric

Average outbound after contact work time

Average time that agents spent doing After Contact Work (ACW) for an outbound contact.
**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 (p. 206)` and `DequeueTimestamp (p. 206)` (from the CTR) for abandoned contacts.

A contact is considered abandoned if it was removed from a queue but not answered by an agent or queued for callback.

**Average queue answer time**

Average time that contacts waited in the queue before being answered by an agent. This is the average of `Duration (p. 206)` (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 don't start in a contact flow, so outbound contacts aren't included.

**Contact handle time**

Total time that an agent spent on contacts, including `Customer Hold Time (p. 198)` and `After contact work time (p. 191)`. This includes any time spent on contacts while in a custom status.
Tip
If you want to exclude the amount of time spent in a custom status, see Agent on contact time (p. 192).

Type: String (hh:mm:ss)
Category: CTR-driven metric

Contacts abandoned
Count of contacts disconnected by the customer while in the queue. Contacts queued for callback are not counted as abandoned. When you create customized historical reports, to include this metric, on the Groupings tab choose either Queue or Phone Number.

Type: Integer
Category: CTR-driven metric

Contacts abandoned in X seconds
Count of contacts disconnected by the customer while in the queue for 0 to X seconds. The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

Type: Integer
Category: CTR-driven metric

Contacts agent hung up first
Count of contacts disconnected where the agent disconnected before the customer.

Type: Integer
Category: CTR-driven metric

Contacts answered in X seconds
Count of contacts that were answered by an agent between 0 and X seconds of being placed in the queue, based on the value of EnqueueTimestamp (p. 206). The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

Type: Integer
Category: CTR-driven metric

Contacts consulted
Count of contacts handled by an agent who consulted with another agent in Amazon Connect. The agent interacts with the other agent, but the customer is not transferred to the other agent.

Type: Integer
Category: CTR-driven metric

Contacts handled
Count of contacts that were connected to an agent.

It doesn’t matter how the contact got to the agent. It could be a customer calling your contact center, or an agent calling the customer. It could be a contact transferred from one agent to another. It could be a contact where the agent answered it, but then they weren’t sure what to do and they transferred the contact away again. As long as the agent was connected to the contact, it increments Contacts handled.
Type: Integer
Category: CTR-driven metric

**Contacts handled incoming**

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

Type: Integer
Category: CTR-driven metric

**Contacts handled outbound**

Count of outbound contacts that were handled by an agent. This includes contacts that were initiated by an agent using the CCP.

Type: Integer
Category: CTR-driven metric

**Contacts hold agent disconnect**

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

Type: Integer
Category: CTR-driven metric

**Contacts hold customer disconnect**

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

Type: Integer
Category: CTR-driven metric

**Contacts hold disconnect**

Count of contacts disconnected while the customer was on hold. This includes both contacts disconnected by the agent and contacts disconnected by the customer.

Type: Integer
Category: CTR-driven metric

**Contacts incoming**

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

Type: Integer
Category: CTR-driven metric

**Contacts missed**

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

When you add this to a historical metrics report, it appears under the column named Agent non-response.
Type: Integer
Category: Agent activity-driven metric

**Contacts put on hold**

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

Type: Integer
Category: CTR-driven metric

**Contacts queued**

Count of contacts placed in the queue.

Type: Integer
Category: CTR-driven metric

**Contacts transferred in**

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

Type: Integer
Category: CTR-driven metric

**Contacts transferred in from queue**

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

Type: Integer
Category: CTR-driven metric

**Contacts transferred out**

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

Type: Integer
Category: CTR-driven metric

**Contacts transferred out external**

Count of contacts that an agent transferred from the queue to an external source, such as a phone number other than the phone number for your contact center.

Type: Integer
Category: CTR-driven metric

**Contacts transferred out from queue**

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

Type: Integer
Category: CTR-driven metric

**Contacts transferred out internal**

Count of contacts for the queue that an agent transferred to an internal source, such as a queue or another agent. An internal source is any source that can be added as a Quick Connect.
Customer hold time

Total time that customers spent on hold after being connected to an agent. This includes time spent on a hold when being transferred, but does not include time spent in a queue.

Type: String (hh:mm:ss)

Error status time

For a specific agent, the total time contacts were in an error status. This metric can't be grouped or filtered by queue.

Type: String (hh:mm:ss)

Maximum queued time

The longest time that a contact spent waiting in the queue. This includes all contacts added to the queue, even if they were not connected with an agent, such as abandoned contacts.

Type: String (hh:mm:ss)

Non-Productive Time

Total time that agents spent in a custom status (p. 44). That is, their CCP status is other than Available or Offline.

This metric doesn't mean that the agent was spending their time unproductively.

Tip

Agents can handle contacts while their CCP status is set to a custom status. For example, agents can be On contact or doing ACW while their CCP is set to a custom status. This means it's possible for agents to be counted as On contact and NPT at the same time.

This metric can't be grouped or filtered by queue.

Type: String (hh:mm:ss)

Occupancy

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

\[
\frac{\text{Agent Handle Time (p. 193)}}{\text{Agent Handle Time (p. 193)} + \text{Agent Idle Time (p. 191)}} \times 100
\]

Type: String

Min value: 0.00%

Max value: 100.00%
Online time

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

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Service level X seconds

Percentage of contacts removed from the queue between 0 and X seconds after being added to it. A contact is removed from a queue when the following occurs: an agent answers the contact, the customer abandons the contact, or the customer requests a call back. The possible values for X are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600. This percentage is calculated as follows:

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

Type: String

Min value: 0.00%

Max value: 100.00%

Category: CTR-driven metric

Contact Search

You can search for contacts as far back as two years ago, 14 days at a time.

The search results for a given query are limited to the first 10K results returned.

When you filter by Contact ID, only results for that specific contact will be returned and other criteria are ignored. For example, say you search for Contact ID 12345 and agent login Jane Doe. Results for Contact ID 12345 will be returned regardless of whether Jane Doe was the agent.

To search contacts

1. Log in to Amazon Connect with a user account that is assigned the CallCenterManager security profile, or one that is enabled for the Contact search permission.
2. In Amazon Connect choose Metrics and quality, Contact search.
3. Use the filters on the page to narrow your search. For date, you can search up to 14 days at a time.
4. To see additional columns in your search results, expand Additional fields to choose what other data you want to view. Choose Apply to view the columns.

Tip

To see if a conversation was recorded, you need to be assigned to a profile that has Manager monitor permissions. If a conversation was recorded, by default the search result will indicate so with an icon in the Recording column. You won't see this icon if you don't have permission to review the recordings.

View a CTR in the UI

To view a CTR in the UI, do a contact search. Contact IDs will be returned. Click an ID to view the CTR for the contact.
The following image shows part of a CTR in the UI. This portion is for a chat.

- For chats, the initiation method is always API.
- The chat transcript is visible in the UI.

Contact Trace Records Data Model

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

**Tip**

Amazon Connect delivers CTRs at least once. CTRs may be delivered again for multiple reasons, such as new information arriving after initial delivery. If you're building a system that consumes CTR export streams, be sure to include logic that checks for duplicate CTRs for a contact. Use the `LastUpdateTimestamp` property to determine if a copy contains new data than previous copies. Then use the `ContactId` property for deduplication.
Agent

Information about the agent 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.

Type: Integer
Min value: 0

**AfterContactWorkEndTimestamp**

The date and time when the agent stopped doing After Contact Work for the contact.

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

**AfterContactWorkStartTimestamp**

The date and time when the agent started doing After Contact Work for the contact.

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. 202)

**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. 207)

Username

The username of the agent.
Type: String
Length: 1-100

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. 202)

Level2

The group at level two of the agent hierarchy.
Type: AgentHierarchyGroup (p. 202)

Level3

The group at level three of the agent hierarchy.
Type: AgentHierarchyGroup (p. 202)
Level 4

The group at level four of the agent hierarchy.

Type: AgentHierarchyGroup (p. 202)

Level 5

The group at level five of the agent hierarchy.

Type: AgentHierarchyGroup (p. 202)

ContactTraceRecord

Information about a contact.

Agent

If this contact successfully connected to an agent, this is information about the agent.

Type: Agent (p. 201)

AgentConnectionAttempts

The number of times Amazon Connect attempted to connect this contact with an agent.

Type: Integer

Min value: 0

Attributes

The contact attributes, formatted as a map of keys and values.

Type: Attributes

Members: AttributeName, AttributeValue

AWSAccountId

The ID of the AWS account that owns the contact.

Type: String

AWSContactTraceRecordFormatVersion

The record format version.

Type: String

Channel

How the customer reached your contact center.

Valid values: Voice, Chat

ConnectedToSystemTimestamp

The date and time the customer endpoint connected to Amazon Connect. 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. 205)

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. 206)

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. 206)

Recording

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

Type: RecordingInfo (p. 206)

Recordings

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

Type: RecordingInfo (p. 206)

Note
The first recording for a contact will appear in both the Recording and Recordings sections of the CTR.

SystemEndpoint

The system endpoint. For INBOUND, this is the phone number that the customer dialed. For OUTBOUND, this is the caller ID phone number that Amazon Connect used to dial the customer.

Type: Endpoint (p. 205)

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. 205)

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 | NULL

**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

---

**How to Identify Abandoned Contacts**

An abandoned contact refers to a contact that was disconnected by the customer while in queue. This means that they weren't connected to an agent.

The CTR for an abandoned contact has a **Queue**, and an **Enqueue Timestamp** because it was enqueued. It won't have a **ConnectedToAgentTimestamp**, or any of the other fields that populate only after the contact has been connected to an agent.
Using the CCP (the Agent UI)

Agents use the Amazon Connect Contact Control Panel (CCP) to interact with customer contacts. It's how they receive calls, chat with contacts, transfer them to other agents, put them on hold, and perform other key tasks.

Large businesses often choose to customize their CCP. For example, they might want to integrate it with a CRM. However, this section describes how CCP works before it is customized.

We recently released an updated CCP. It provides a single interface for agents to manage both voice and chat contacts. Even if your business is currently taking only voice contacts, we recommend using the updated CCP.

The following image shows the CCP.

Contents
- Launch the CCP (p. 209)
- Log In and Log Out of the Amazon Connect CCP (p. 209)
Launch the CCP

The URL to launch the Contact Control Panel (CCP) is:

https://name of your instance.awsapps.com/connect/ccp-v2/

With this updated CCP, your agents can manage both voice and chat contacts from this single interface.

As the administrator, you can also launch the CCP directly from the Amazon Connect console. Just choose the phone icon in the upper right corner.

To provide agents the ability to launch the CCP from their desktop and start handling contacts, there are a few things you need to do:

- Add agents as users to the instance. For more information, see Manage Users in Amazon Connect (p. 135).
- Configure permissions for the agents. By default, agents assigned to the Agent security profile can access the CCP and make outbound calls. But you can create a custom security profile and add additional permissions. For more information, see Assign Permissions: Security Profiles (p. 136).
- Give agents the URL the CCP.
- Provide agents with their user name and password so that they can log in to the CCP.

We recommend telling agents to bookmark the URL to the CCP for more convenient access.

Agents can use the CCP with a softphone on their computer, or a deskphone. If they’re using a softphone, they must use Chrome or Firefox for their web browser. For more information, see Grant Microphone Access in Chrome or Firefox (p. 47).

Log In and Log Out of the Amazon Connect CCP

Before you can log in to the Contact Control Panel (CCP), your administrator must give you the following information:

- A link to the CCP. It looks something like this: https://name of your center.awsapps.com/connect/ccp-v2/.
- Your agent ID.
- Your agent password.

After you have that information, here’s how to log in and get started.

1. Ensure that your USB headset is securely connected to your computer.
2. Using Chrome or Firefox, open the CCP by using the URL that you received from your administrator.
3. Enter your agent ID and password, and then choose Sign In.
4. If you are prompted to allow access to your microphone and speaker, choose Allow.

You're all set to go!

Log Out of the Amazon Connect CCP

**Important**
Closing the CCP windows doesn't automatically sign out agents. Amazon Connect still tries to route contacts to them. To change this behavior, customize your CCP.

1. At the top of the CCP, select the Change Status dropdown menu.
2. Choose Log out.
Set Your Status to Available

When an agent is ready to handle calls or chats, they need to set their status in the CCP to Available. This tells Amazon Connect they are ready to handle contacts.

Amazon Connect uses information in the agent's routing profile (p. 42) to determine which contacts to route to them.

Chat with Contacts

When you set your status in the CCP to Available, Amazon Connect delivers calls or chats to you, based on the settings in your routing profile (p. 42). An administrator can specify that up to five chat conversations can be routed to you at the same time.

You can't initiate chat conversations from the CCP.

Customers and agents can't send attachments, such as files, through the chat interface.

Tip
Amazon Connect routes contacts to you for only one channel at a time. When you're on a call, you won't be routed a chat conversation. And when you're handling chat conversations, you won't be routed a call.

When a chat contact arrives, here's how you are notified:

1. If you enabled notifications in your browser, you'll get a pop-up notification at the bottom of your screen, like this:
2. If you're on the chat tab, the page displays the name of the contact and a button for you to connect to the chat.

3. If you're on the voice tab, a banner displays the name of the contact and a button for you to connect to the chat.

4. If you're on a chat, and another comes in but you don't accept it, a tab appears indicating the chat was missed.

5. Choose **Accept chat** to connect to the contact.

**Note**
Chat conversations must be accepted manually. There's no auto-accept for these conversations.
What Do the Timers at the Top of the Chat Tabs Mean?

When you're in a chat conversation with a contact, you'll see two timers at the top of the chat tab. These timers tell you:

- How long the contact has been connected to your contact center. This includes the time spent with the bot, if you're using one.
- How long since the last text was sent. This can be either from the customer to the agent, or from the agent to the customer. The timer is reset with each text message.
What Happens to Missed Chats?

Let's say you take a break but forget to change your status in the CCP from Available to Break. Amazon Connect tries to route a chat to you for 15 seconds. Keep in mind that your admin can't configure this amount of time.

After 15 seconds, the contact is counted as Agent non-response (p. 182) in the real-time metrics report and the historical metrics report.

When you return from break and choose the chat tab, you'll see the missed contacts and how long they've been there. Each contact occupies a slot. This way, with all of your slots are occupied, Amazon Connect won't route any more contacts to you.
Transfer Chats to Another Queue or Agent

When a chat is transferred from a bot to an agent or from one agent to another agent, all context is preserved. This context lets the next agent read all previous messages in that contact.

To transfer a customer to another agent or queue
1. Choose the Quick Connect button at the bottom of the CCP page.
2. Choose or search for the agent or queue you want to transfer to, and then choose the transfer button.
3. You'll see a confirmation message. You're now doing After Contact Work for the customer. Choose **Close** to end the contact.
Call Another Agent While on a Chat

Let's say you're chatting with a contact and you want to consult with another agent. While you're on a chat, you can use the updated CCP to make outbound calls and call other agents. However, you and other agents can't receive calls while on a chat.

If you're on a chat and having trouble making an outbound call to another agent, that agent may currently be handling a chat conversation.

Accept Incoming Calls

1. Whenever you set your status in the CCP to Available, Amazon Connect can deliver calls to you, based on the settings in your routing profile (p. 42).
2. When a call arrives, choose the **Accept call** button.

3. Before you're connected to the contact, Amazon Connect announces the name of the originating queue.

4. You're now talking to the contact.

5. If you miss a call, it will look similar to the following image. Choose **Clear contact** so you can accept another call.
Transfer Calls

You can transfer calls to people in a predefined list, called quick connects. You can also transfer calls to phone numbers that you dial.

Initiate a Quick Connect Transfer

To transfer a call to a predefined destination

1. Choose the Quick Connect button on the CCP.
2. Select another agent to transfer the call to, or enter a number.
3. After the call is connected, you can choose Join so you, the caller, and the transfer destination are in a conference call.
4. When the call is joined, you’ll have the option to choose **Leave** to exit the call.
Initiate a Manual Transfer

1. Transfer a call to a phone number by choosing Number pad.
2. Enter the number you want and choose Call.
Manage Transfer a Call

After the transfer has been initiated, the customer is placed on hold and you'll be connected to the transfer destination.
Put all parties on hold.

Places you, the caller, and the transfer destination into a conference.
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
- Use the Check Connectivity Tool (p. 225)
- Common CCP Issues (p. 225)
- Useful Troubleshooting Tools and Information (p. 226)
- Gathering Helpful Information using the Streams API (p. 227)
- Analyzing the Data (p. 227)
- Validation Testing (p. 228)

Use the Check Connectivity Tool

When your agents are experiencing problems with CCP, we recommend you go to their workstation and run the Amazon Connect Check Connectivity Tool.

This tool will check which web browser the agent is running, and whether the microphone has required permissions. Click the Test buttons to check the ports and latency.

Common CCP Issues

The following are common issues encountered when using the Amazon Connect CCP.

- **CCP does not initialize/connect**—The most common causes are missing port/IP allow list entries, not allowing browser microphone access, or not answering your external device. Be sure that you have added to the allow list all IPs covered in the Set Up Your Network (p. 102) section of this guide, and that you have allowed microphone access to your browser when prompted.

- **Periodic connection errors**—The most common cause is network contention, or there may have been an ipranges.json update and the new entries have not been added to the allow list. For more information, see the Set Up Your Network (p. 102) 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. 49) 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. 49)
  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. 49) 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 allow list access**—to verify that IP/port ranges are added to the allow list (also known as
  whitelist) as described in Set Up Your Network (p. 102).

- **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 \([\text{pstn\_latency}]\).

Amazon Connect leverages CloudFront for connectivity. Not all CloudFront ranges are advertised over AWS Direct Connect. This means not all URLs generated by AWS Direct Connect are reachable over a Public Virtual Interface.

- \([\text{redirect\_latency}]\) is the latency resulting in redirecting audio to an external device. This latency can be calculated by measuring \([\text{overall\_latency}]\) once with redirect and once without and take the difference between the two.
- \([\text{forward\_latency}]\) is the latency resulting in forward calls to or from Amazon Connect. This latency can be calculated by measuring \([\text{overall\_latency}]\), 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 [overall_latency].

12. Optionally, to calculate [agent_latency], open the associated Amazon Connect call recording in your audio analysis tool. You should be able to see both the initial tapping sound and the sound when it arrives to the agent at the other end. Take the three deltas and average for your [recording_latency].

\[
\text{[agent_latency]} = \text{[overall_latency]} - \text{[recording_latency]}
\]

Modify the test plan as necessary to fit your use case. As the steps change, the process of recording and analyzing the audio is the same. If you need to test conferences and transfers, take measurements as normal, and then take another measurement when the conference is active with the third party transfer endpoint.

**Interpreting the Test Results**

The impact of increasing [overall_latency] begins to be noticeable at approximately 300ms and can result in crosstalk above 500ms. The impact, and what level of latency is considered acceptable, depends on your use case. For recommended remediation efforts for decreasing latency, see the PSTN and Agent Connection Latency (p. 228).
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. 233).

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. 34).

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>
<tr>
<td>Agent hierarchy groups per instance</td>
<td>250</td>
</tr>
</tbody>
</table>

This limit cannot be increased.
<table>
<thead>
<tr>
<th>Item</th>
<th>Default limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports per instance</td>
<td>500</td>
</tr>
<tr>
<td>Personal saved reports count towards the reports per instance. For example, if one of your supervisors saves a report every day, it will count towards your overall number of saved reports per instance.</td>
<td></td>
</tr>
<tr>
<td>As a best practice, we recommend you implement policies so reports don’t pile up.</td>
<td></td>
</tr>
<tr>
<td>Managers who can listen in on an agent call at the same time</td>
<td>5</td>
</tr>
<tr>
<td>This limit cannot be increased.</td>
<td></td>
</tr>
<tr>
<td>Scheduled reports per instance</td>
<td>50</td>
</tr>
<tr>
<td>Contact Trace Record retention</td>
<td>24 months from the time the associated contact was initiated. This limit cannot be increased.</td>
</tr>
<tr>
<td>You can choose to stream CTRs to Kinesis so you can manage retention and perform advanced analysis.</td>
<td></td>
</tr>
<tr>
<td>Lambda functions</td>
<td>35 functions per Amazon Connect instance</td>
</tr>
<tr>
<td>Amazon Lex bots</td>
<td>50 Amazon Lex bots per Amazon Connect instance</td>
</tr>
<tr>
<td>Concurrent chats per instance</td>
<td>100. This includes chats that are waiting.</td>
</tr>
<tr>
<td>If this is exceeded, the API call fails with a limit exceeded error.</td>
<td></td>
</tr>
<tr>
<td>Active chats per agent</td>
<td>5</td>
</tr>
<tr>
<td>This limit cannot be increased.</td>
<td></td>
</tr>
<tr>
<td>Total duration per chat</td>
<td>25 hours, including wait time</td>
</tr>
<tr>
<td>This limit cannot be increased.</td>
<td></td>
</tr>
<tr>
<td>Characters per chat message</td>
<td>1024</td>
</tr>
<tr>
<td>This limit cannot be increased.</td>
<td></td>
</tr>
<tr>
<td>Concurrent calls per instance</td>
<td>100. If this is exceeded, contacts will get a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.</td>
</tr>
<tr>
<td>Phone Number Porting</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. 34).</td>
</tr>
</tbody>
</table>
Amazon Connect API Throttling Limits

<table>
<thead>
<tr>
<th>Item</th>
<th>Default limit</th>
</tr>
</thead>
</table>
| Country code allow list for Outbound Calls | You can place calls to the following dialing codes when you create a new instance:  
  - Australia  
  - Canada  
  - China  
  - Germany  
  - Hong Kong  
  - Israel  
  - Japan  
  - Mexico  
  - Singapore  
  - Sweden  
  - United States  
  - United Kingdom†  

† 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.

Amazon Connect API Throttling Limits

Amazon Connect throttling limits are by account, not by user and not by instance. For example:

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

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

- For the `GetMetricData` and `GetCurrentMetricData` operations, a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second. These limits cannot be increased.
- For all other operations, a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.

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

- `CreateParticipantConnection`, `DisconnectParticipant`, and `GetTranscript`: a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.
- `SendMessage` and `SendEvent`: a RateLimit of 10 requests per second, and a BurstLimit of 15 requests per second.
Additional Resources for Amazon Connect

In addition to using the contents of this guide, you can learn more about Amazon Connect by using the online resources listed in this topic.

Amazon Connect Service API Documentation

The Amazon Connect Service API Documentation provides details about all the operations, types, inputs and outputs, and error codes.

Amazon Connect Participant Service API

The Amazon Connect Participant Service API provides details about the APIs used by chat participants, such as agents and customers.

Amazon Connect Streams

Use the Amazon Connect Streams documentation to integrate your existing web applications with Amazon Connect. Streams gives you the power to embed the Contact Control Panel (CCP) UI components into your page, and/or handle agent and contact state events directly giving you the power to control agent and contact state through an object oriented event driven interface. You can use the built in interface or build your own from scratch: Streams gives you the power to choose.

Amazon Connect Chat SDK and Sample Implementations

See the Amazon Connect Chat SDK and Sample Implementations for examples of how to enable your app to engage with Amazon Connect chat.
Release Notes

To help you keep track of the ongoing updates and improvements to Amazon Connect, we publish release notices that describe recent changes.

Updates
- November 2019 Update (p. 235)
- October 2019 Update (p. 236)
- June 2019 Update (p. 236)
- May 2019 Updates (p. 237)
- April 2019 Updates (p. 237)
- March 2019 Update (p. 237)
- February 2019 Updates (p. 238)
- January 2019 Updates (p. 239)
- December 2018 Updates (p. 239)
- November 2018 Updates (p. 240)
- October 2018 Updates (p. 240)
- September 2018 Updates (p. 241)
- August 2018 Updates (p. 241)
- July 2018 Updates (p. 242)
- June 2018 Updates (p. 243)
- April and May 2018 Updates (p. 244)

November 2019 Update

The following updates were released in November 2019:

Omnichannel Support
- Added support for chat communications. For more information, see Concepts (p. 5).

Metrics
- For a description of changes, see What's New in Metrics (p. 171).

Contact Flows

Added the following contact flow blocks:
- Wait
• Set disconnect flow

Updated the following contact flow blocks for chat:

• Play prompt
• Get customer input
• Store customer input
• Set recording behavior

User Management

• Added that you can use AWS Identity and Access Management (IAM) with Amazon Connect. For more information, see Controlling Access with AWS Identity and Access Management (p. 139).

Live Media Streaming

• Added that you can capture customer audio for the entire interaction with your contact center. For more information, see Capture Customer Audio: Live Media Streaming (p. 122).

API

• Added StartChatContact, ListTagsForResource, TagResource, UntagResource to the Amazon Connect Service API.
• Added the Amazon Connect Participant Service API. These APIs are used chat participants, such as agents and customers.

Contact Control Panel (CCP)

• Updated the CCP so it supports chat. For more information, see Using the CCP (the Agent UI) (p. 208).

October 2019 Update

The following update was released in October 2019:

Metrics

• The real time metric On call is now incremented whenever an agent is handling a contact who is connected, on hold, in After Contact Work, or the agent is dialog out to a customer.

  This metric is available in the Queues tables and Routing Profile tables on the Real time metrics page. It’s also returned by the GetCurrentMetricData API as AGENTS_ON_CALL.

June 2019 Update

The following update was released in June 2019:
Contact Flows

- Added contact flow versioning so you can choose between a saved or published version when you roll back.

May 2019 Updates

The following updates were released in May 2019:

Metrics and Reporting

- Improved the error messages you might encounter when creating, editing, or deleting a scheduled report.
- In the Historical metrics report UI, changed Contacts missed to Agent non-response. This metric appears as Contacts missed in scheduled reports and exported CSV files.
- In the agent event stream, fixed the formatting of the timestamp millisecond so you can better order and analyze the data. To learn more, see Amazon Connect Agent Event Streams (p. 150).

Contact Control Panel

- Resolved an issue where calling a destroy action (such as connection.destroy) using the Amazon Connect Streams API resulted in different behavior depending on which leg of the conversation it was called from: the agent or the customer. Now calling a destroy action results in the same behavior for both: a busy conversation is moved to After Call Work (ACW) and a conversation in any other state is cleared. If you used the native Contact Control Panel instead of the Amazon Connect Streams API, you weren't impacted by this issue.

April 2019 Updates

The following updates were released in April 2019:

Contact Control Panel

- Resolved an issue where the hold flow didn't run in this case:
  - The agent missed a call and then set themselves back to Available.
  - Then they were re-routed the same call.
  - The agent put that customer on hold while handling the call.

  However, taking the customer off hold worked as expected and no other impact occurred.
- Resolved an issue where the Amazon Connect Streams API returned softphoneAutoAccept = FALSE even though Auto-Accept Call was enabled for the agent.

March 2019 Update

The following updates were released in March 2019:
Metrics and Reporting

- Improved the error messages you might encounter when running real-time metrics reports. For example, if you manually configure a real-time metrics report to contain more than 100 queues, we'll display this message: “You've hit the maximum limit of 100 queues. Please reconfigure your report to contain no more than 100 queues.” To learn more, see No Metrics or Too Few Rows in a Queues Report? (p. 179)

Contact Control Panel

- Resolved an issue where, in rare cases, an agent already handling an outbound call could have been incorrectly presented with an additional queued callback, even though they are only allowed to handle one contact at a time. Since that agent would have been on contact and not idle, the agent wouldn't have been able to accept the queued callback.

  In these cases, the outbound call was not impacted; the agent wouldn't have noticed any differences in the CCP. The callback was presented to another agent instead of being dropped.

February 2019 Updates

The following updates were released in February 2019:

Updates by category

- Contact Routing (p. 238)
- Contact Flows (p. 238)
- Metrics and Reporting (p. 238)
- Contact Control Panel (CCP) (p. 239)

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. 239)
- Contact Flows (p. 239)
- Metrics and Reporting (p. 239)

**Contact Routing**

Resolved an issue where in rare cases agent transfers were failing.

**Contact Flows**

Resolved an issue where agent transfers were failing.

Resolved an issue that resulted in periodic delays in publishing contact flow logs.

**Metrics and Reporting**

Resolved an issue in real-time metrics reports where the page showed the wrong calculation for `Avg queue answer time`.

Resolved an issue where some events were missing from an agent event stream.

**December 2018 Updates**

The following updates were released in December 2018:

**Updates by category**
- Metrics and Reporting (p. 239)
- Contact Control Panel (CCP) (p. 240)

**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. 240)
• Contact Flows (p. 240)
• Metrics and Reporting (p. 240)

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. 241)
- **Metrics and Reporting** (p. 241)
- **API** (p. 241)

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

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

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

## September 2018 Updates

The following updates were released in September 2018:

### Updates by category
- **General** (p. 241)
- **API** (p. 241)

### 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

- 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. 242)
- General (p. 242)
- Metrics and Reporting (p. 243)
- Contact Flows (p. 243)

**New Features**

- Initiate an Outbound Call (p. 70)
- Add an Amazon Lex Bot (p. 108)
- User Management APIs
- Manage Contact in a Queue Using a Transfer to Queue Block (p. 66)

**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. 243)
- Telephony and Voice (p. 243)
- Contact Flows (p. 243)
- Metrics and Reporting (p. 244)
- Contact Control Panel (CCP) (p. 244)

**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. 70).
• Released contact attributes for system metrics, including a new Get metrics block in contact flows. For more information, see How to Use System Metric Attributes (p. 93).

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. 244)
- Telephony and Voice (p. 244)
- Contact Flows (p. 245)
- Metrics and Reporting (p. 245)
- Contact Control Panel (CCP) (p. 245)

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 live media streaming</td>
<td>For more information, see Capture Customer Audio: Live Media Streaming (p. 122).</td>
<td>November 21, 2019</td>
</tr>
</tbody>
</table>
| Added information about chat                                           | For more information, see Chat (p. 8).
<p>|                                                                       | Also added these topics: Best Practices for Amazon Connect (p. 17), About Agent Status (p. 174), About Contact States (p. 175), and Additional Resources for Amazon Connect (p. 234). | November 21, 2019  |
| Added topic on using IAM                                               | For more information, see Controlling Access with AWS Identity and Access Management (p. 139).        | November 14, 2019  |
| Added dimensions                                                       | Added dimensions to the Amazon Connect metrics sent to CloudWatch. See CloudWatch Metrics for Your Amazon Connect Instance (p. 165). | October 22, 2019   |
| Added a networking topic                                               | Consolidated networking content into Set Up Your Network (p. 102). Updated the guidance.            | September 30, 2019 |
| Updated metrics topics                                                 | Improved the descriptions of the real-time metrics definitions. Added categories to the historical metrics definitions. | August 30, 2019    |
| Re-organized the content                                               | Re-organized the content so it's task-based.                                                        | July 19, 2019      |
| Added information about the updated <strong>Transfer to phone number</strong> block | 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. 65). | February 18, 2019  |</p>
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding information about live media streaming for customer audio streams</td>
<td>You can capture customer audio during interactions with your contact center and send it to a Kinesis video stream. For more information, see Capture Customer Audio: Live Media Streaming (p. 122).</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Added content about agent queues</td>
<td>You can use agent queues to route calls directly to a specific agent. For more information, see Transfer Contacts Directly to a Specific Agent (p. 67).</td>
<td>December 21, 2018</td>
</tr>
<tr>
<td>Added information about using Amazon Connect in the Asia Pacific (Tokyo) Region.</td>
<td>For more information, Claim Phone Numbers for Amazon Connect in the Asia Pacific (Tokyo) Region (p. 36).</td>
<td>December 10, 2018</td>
</tr>
<tr>
<td>Added information about how to determine agent ACW time from agent event streams</td>
<td>For more information, see Determine How Long an Agent Spends Doing ACW (p. 153).</td>
<td>October 30, 2018</td>
</tr>
<tr>
<td>Added troubleshooting and best practices</td>
<td>Troubleshooting Issues with the CCP (p. 225) covers best practices for agent connectivity using the CCP and troubleshooting connectivity and call quality issues in Amazon Connect.</td>
<td>October 18, 2018</td>
</tr>
<tr>
<td>Added information about service-linked roles in Amazon Connect</td>
<td>For more information, see Use Service-Linked Roles for Amazon Connect (p. 137).</td>
<td>October 17, 2018</td>
</tr>
<tr>
<td>Added information about queue to queue transfers</td>
<td>You can use the new options of the Transfer to queue block to enable transferring calls that are already in a queue to another queue. For more information, see Manage Contact in a Queue Using a Transfer to Queue Block (p. 66).</td>
<td>July 31, 2018</td>
</tr>
<tr>
<td>Added information about the Call phone number block</td>
<td>Updated the content about contact flows to include the new Call phone number block, including how to use the block in a contact flow. For more information, see Initiate an Outbound Call (p. 70).</td>
<td>July 2, 1018</td>
</tr>
<tr>
<td>Added information about contact attributes and the Get queue metrics block</td>
<td>For more information, see Use Amazon Connect Contact Attributes (p. 84).</td>
<td>June 18, 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 new metrics sent to Amazon CloudWatch Logs.</td>
<td>CloudWatch Metrics for Your Amazon Connect Instance (p. 165) 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. 21).</td>
<td>March 30, 2018</td>
</tr>
<tr>
<td>Added information about agent call transfers</td>
<td>You can enable call transfers from an agent to another agent, to a queue, or to an external number.</td>
<td>December 10, 2017</td>
</tr>
<tr>
<td>Added information about manager listen-in</td>
<td>You can configure and enable a manager to listen in on agent calls. For more information, see Monitor Live Conversations (p. 143).</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. 163).</td>
<td>November 16, 2017</td>
</tr>
<tr>
<td>Added information about contact flow import/export</td>
<td>For more information, see Import/Export Contact Flows (p. 71).</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. 150).</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. 34).</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Added information about Login/Logout reports</td>
<td>For more information, see Login/Logout Reports (p. 146).</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>